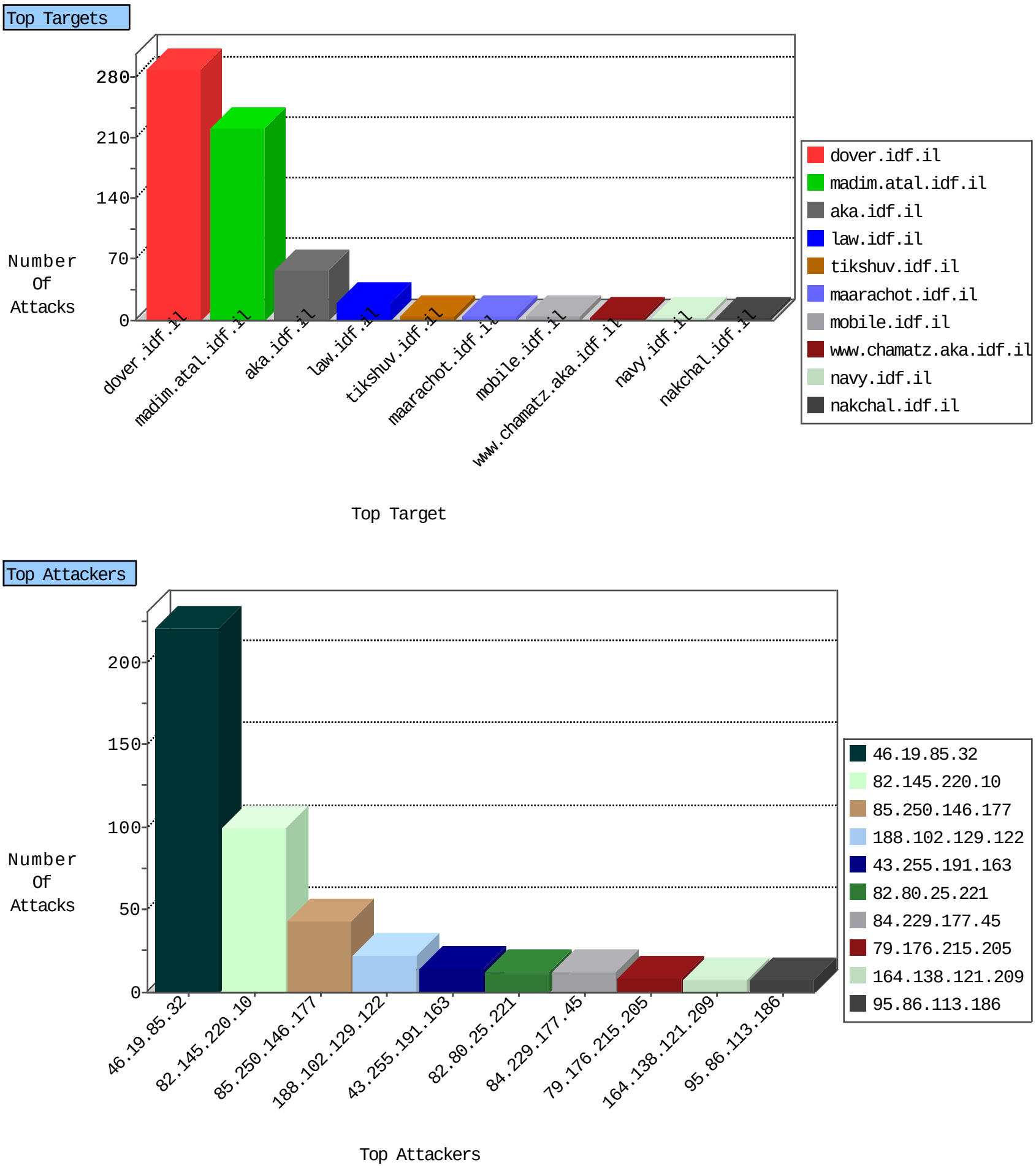
04-25-2015-23:03:03 to 04-26-2015-00:03:03

IDF Under Attack
04-25-2015-23:03:03



04-25-2015-23:03:03 to 04-26-2015-00:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1030
220.181.108.105	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	393
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	193
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	128
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	10
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6
37.46.39.97	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
79.181.24.189	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
110.169.62.60	Thailand	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

04-25-2015-23:03:03 to 04-26-2015-00:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.125.222.161	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
89.138.80.97	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.32	Israel	147.237.0.19	madim.atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.164	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1

04-25-2015-23:03:03 to 04-26-2015-00:03:03

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.65.12	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.4	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.66	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
37.142.226.237	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.163	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
136.243.5.219	Germany	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	China	147.237.76.31	nakchal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
43.255.191.163	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
113.21.226.56	New Zealand	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
87.68.162.84	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.183.128.6	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
58.20.54.249	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.238	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
43.255.191.163	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
128.199.167.194	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
61.183.128.6	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	Turkey	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
85.204.147.138	Romania	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.140.209	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.113	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.235	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
43.255.191.163	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1

04-25-2015-23:03:03 to 04-26-2015-00:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.145.220.10	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	100
85.250.146.177	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
188.102.129.122	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
84.229.177.45	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
176.12.149.64	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
82.102.136.68	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
80.230.14.203	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
37.26.148.229	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
93.173.234.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
207.46.13.52	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
85.64.216.75	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
207.46.13.95	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
84.110.2.108	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
79.179.20.181	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
149.78.186.96	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
46.19.85.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
109.66.60.228	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
79.181.24.189	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
70.120.75.223	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
109.67.114.241	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
95.86.104.108	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
81.218.170.209	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
98.102.163.137	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
5.29.90.117	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
109.65.51.251	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
79.179.107.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
37.26.148.185	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
162.243.2.119	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
86.178.85.49	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
46.121.135.50	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
199.102.52.253	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
85.64.58.110	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	1
173.46.233.232	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
82.166.114.5	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
176.12.142.8	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
84.109.160.11	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
79.177.164.224	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
117.204.144.246	India	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
85.65.80.135	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.32	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 46.19.85.32	Block	219
79.176.215.205	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
164.138.121.209	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
95.86.113.186	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	7
95.86.83.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
79.178.209.44	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	4
2.52.2.113	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
78.46.203.72	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.98	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
188.165.15.13	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.13	Block	2
37.26.148.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
87.68.147.110	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.89	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
91.200.12.74	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11845-en/dover.aspx/trackback/	Block	1
207.46.13.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/034.stm	Block	1
76.73.71.185	United States	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
66.249.78.51	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
157.55.39.127	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	Block	1
46.19.85.146	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
95.86.123.137	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
84.229.133.225	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
178.141.171.108	Russian Federation	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/images/0108	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.59	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/enlarge.asp	Block	1
31.173.240.126	Romania	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/163-7183-en/patzar.aspx	Block	1
94.230.86.217	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
213.151.51.82	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.179	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/doctor	Block	1
134.249.53.8	Ukraine	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
85.64.84.49	Israel	147.237.0.19	madim.atal.idf.i	Multiple Unauthorized URL Access from 85.64.84.49	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18362	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/×ž×™×œ×•×?×™×?/contact/	Block	1
66.249.64.66	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/mobile/	Block	1
134.249.65.181	Ukraine	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	1
188.165.15.13	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/born5.stm	Block	1
66.249.81.228	Israel	147.237.76.31	nakchal.idf.il	URL is Above Root Directory www.nakhal.idf.il/../favicon.ico	Block	1
157.55.39.8	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.69	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
46.19.85.32	Israel	147.237.0.19	madim.atal.idf.i	Too Many 404: Response Code per Session	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/unitfs.asp	Block	1
167.114.64.100	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
89.138.226.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.1	Block	1
76.73.71.185	United States	147.237.77.74	law.idf.il	E-mail collector robots 14	Block	1

04-25-2015-23:03:03 to 04-26-2015-00:03:03