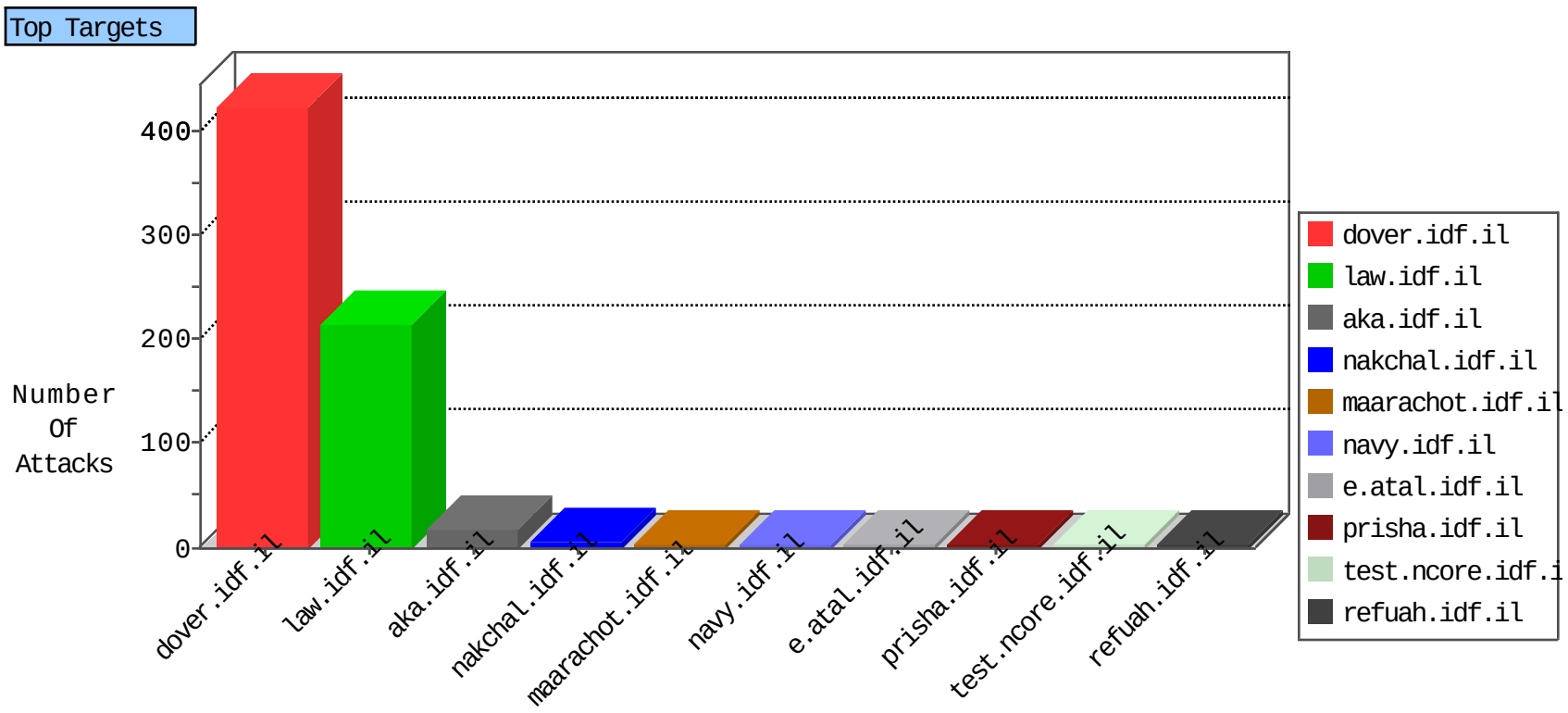
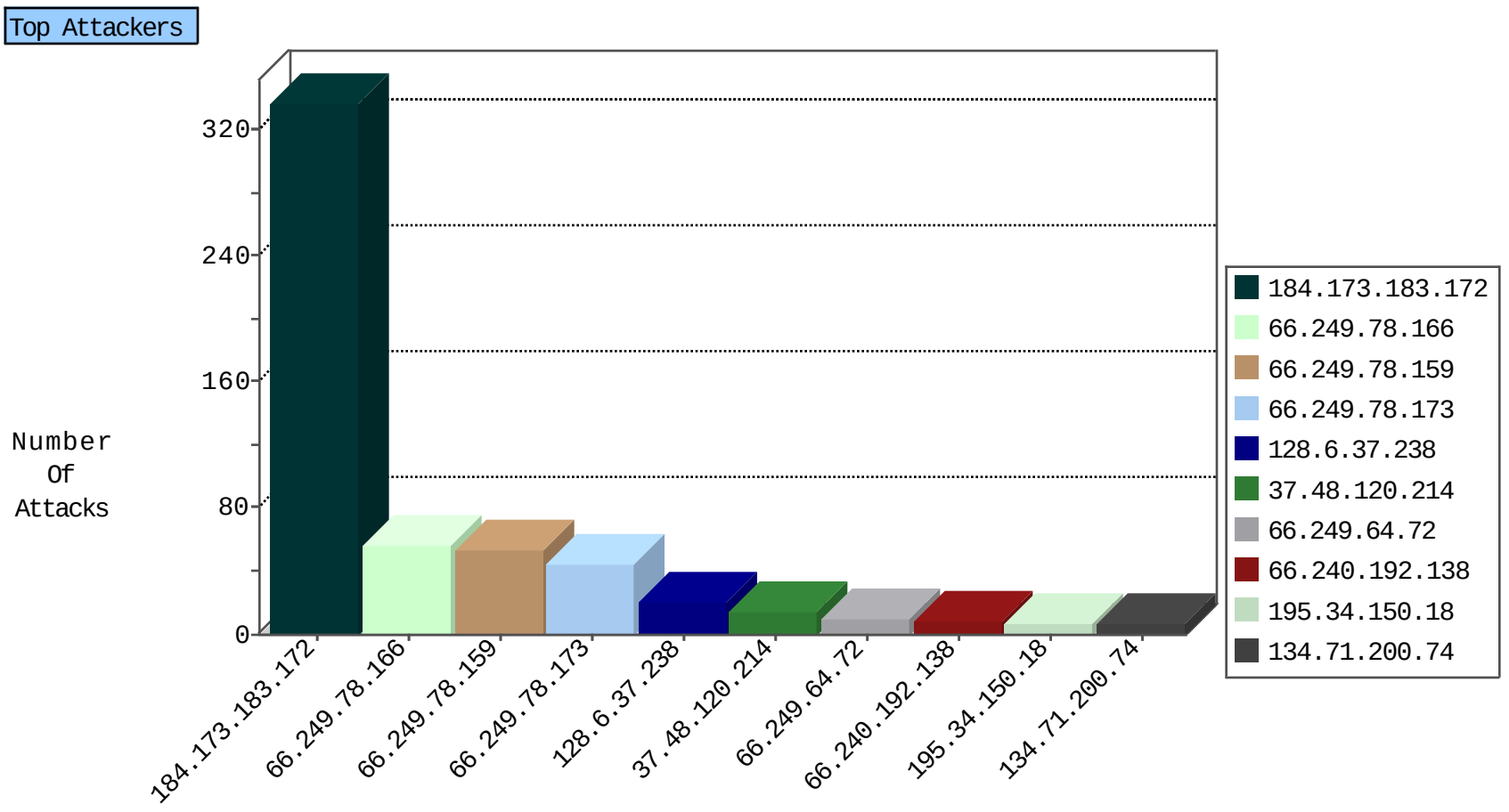
05-05-2015-04:03:06 to 05-05-2015-05:03:06

IDF Under Attack
05-05-2015-04:03:06

Top Targets



Top Attackers



05-05-2015-04:03:06 to 05-05-2015-05:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.90	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	223
220.181.108.179	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	69
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
157.14.230.110	Japan	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	2
104.192.0.20		147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.58	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
149.78.154.69	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
104.192.0.20		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

05-05-2015-04:03:06 to 05-05-2015-05:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	207
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	130
199.203.170.141	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
188.138.9.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	2
66.240.236.119	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1

05-05-2015-04:03:06 to 05-05-2015-05:03:06

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
66.249.78.96	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.65.46	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
201.239.118.143	Chile	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
188.95.158.198	Ukraine	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
119.90.139.72	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
119.90.139.72	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.67	China	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.5.191		147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
201.239.118.143	Chile	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
188.95.158.198	Ukraine	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
119.90.139.72	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.67	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1

05-05-2015-04:03:06 to 05-05-2015-05:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
128.6.37.238	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
134.71.200.74	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
170.140.105.16	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.64.72	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
50.177.0.227	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
98.136.188.185	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
99.171.138.199	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
73.9.99.73	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
188.120.148.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.166.167.129	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
188.120.148.134	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
109.67.33.183	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
184.105.247.244	United States	147.237.76.34	yohalan.idf.il		drop	drop	1
66.249.64.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
108.61.122.156	United States	147.237.0.33	idf.il		drop	drop	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
85.130.244.197	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
108.61.122.156	United States	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	1
46.161.41.199	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
173.93.224.224	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
125.202.25.184	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
54.177.31.205	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

05-05-2015-04:03:06 to 05-05-2015-05:03:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	46
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	43
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	38
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	5
192.187.124.251	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.187.124.251	Block	3
157.55.39.204	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	2
213.151.58.251	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	2
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	2
207.46.13.101	United States	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	Distributed Suspicious Response Code	Block	2
66.249.64.70	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
103.250.208.64	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1008-en/+navmenu.qc+	Block	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	1
188.165.15.176	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1120-2.stm	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/news/kamlar/mishpaha.jpg+	Block	1
192.187.124.251	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/admin/assetmanager/assetmanager.asp	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.204	Block	1
142.54.161.131	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 142.54.161.131	Block	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	1
222.92.74.98	China	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
190.74.193.186	Venezuela	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/en	Block	1
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1217-6.stm	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/humanitarianarchive.stm	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_moreinfo.asp	Block	1
204.236.101.223	Bahamas	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
180.76.5.170	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.88	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
192.187.124.251	United States	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
66.249.64.65	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/m/	Block	1
157.55.39.158	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
188.165.15.99	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.99	Block	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.66	Block	1
66.249.75.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/templates/sendtofriend/sendtofriend.aspx	Block	1
192.187.124.251	United States	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 192.187.124.251	Block	1
66.249.64.68	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_text.asp	Block	1
207.46.13.101	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.101	Block	1
188.165.15.99	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/april/19.stm	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

05-05-2015-04:03:06 to 05-05-2015-05:03:06