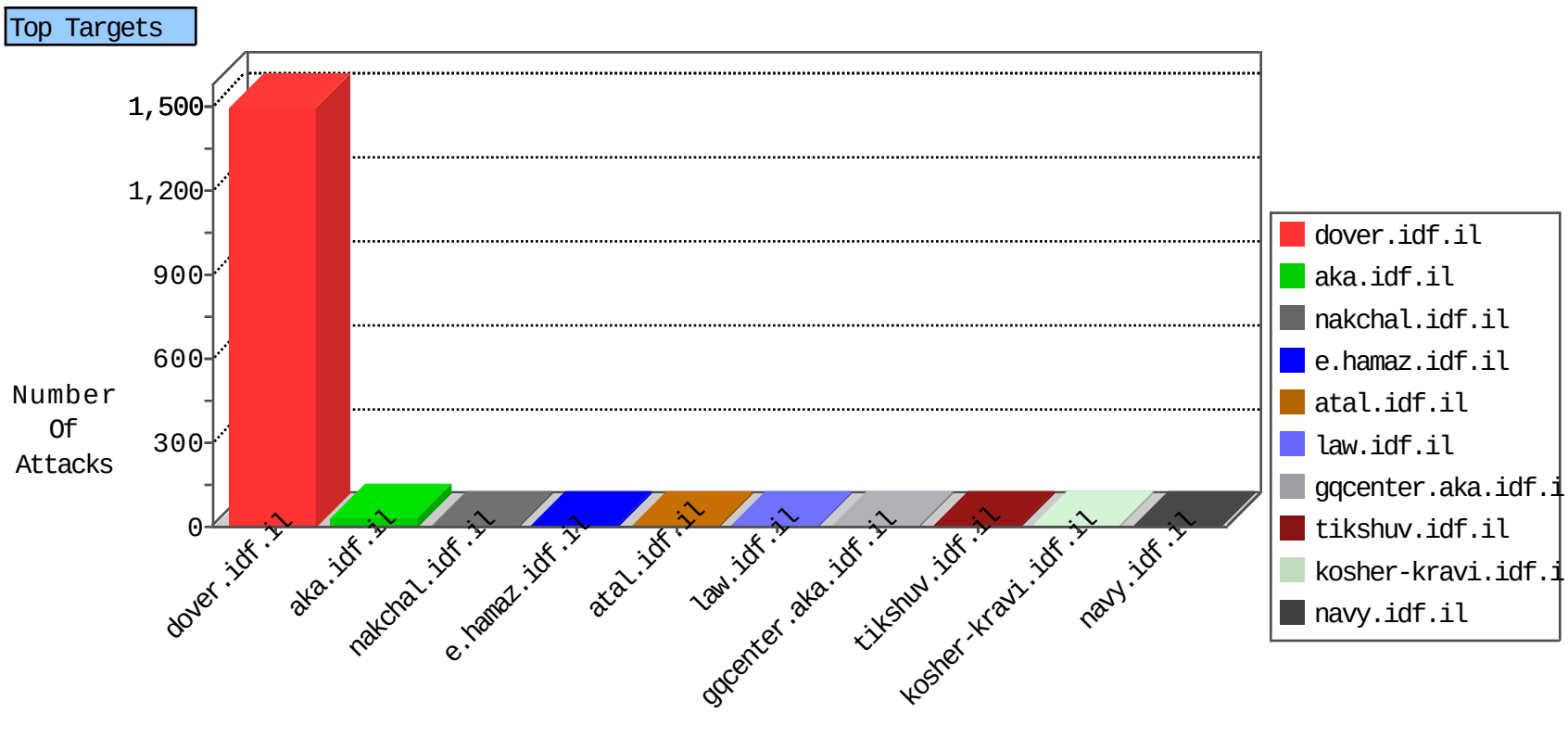
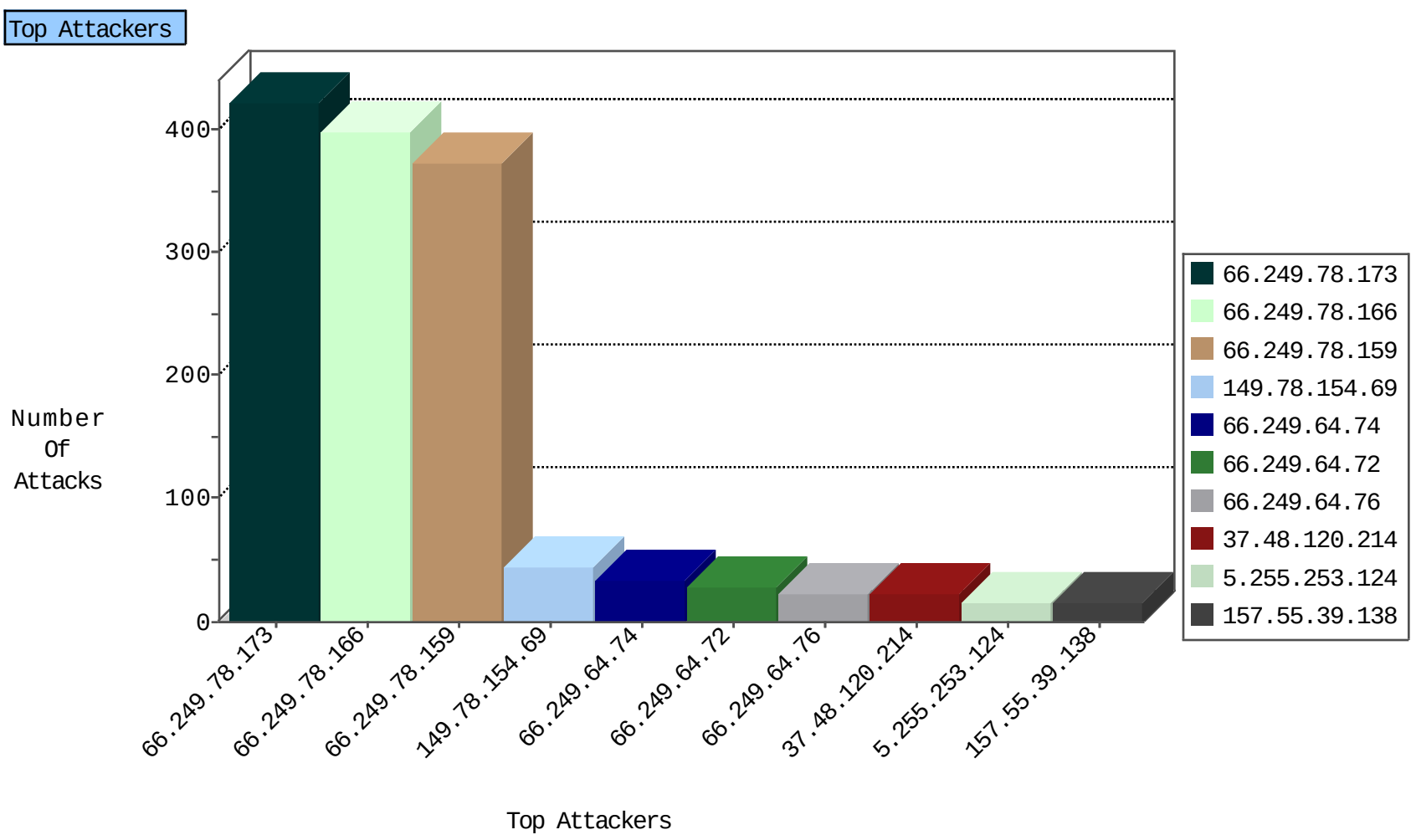
05-02-2015-06:03:07 to 05-02-2015-07:03:07

IDF Under Attack
05-02-2015-06:03:07

Top Targets



Top Attackers



05-02-2015-06:03:07 to 05-02-2015-07:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
84.101.132.119	France	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2
157.55.39.61	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
46.229.164.113	United States	147.237.0.34	tikshuv.idf.il	network flood IPv4 TCP-FIN-ACK	drop	1
192.3.206.130	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

05-02-2015-06:03:07 to 05-02-2015-07:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.25.43.94	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.148	gqcenter.aka.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
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1

05-02-2015-06:03:07 to 05-02-2015-07:03:07

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
66.249.78.29	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.69.66	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.67	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.178	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
221.229.166.28	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
59.41.39.125	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
205.189.20.55	Canada	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
59.41.39.125	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
119.92.202.251	Philippines	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1
103.23.76.113	Singapore	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.178	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
205.189.20.55	Canada	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
59.41.39.125	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
119.92.202.251	Philippines	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
91.238.134.92	Poland	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

05-02-2015-06:03:07 to 05-02-2015-07:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	78
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	76
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	76
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	44
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
66.249.78.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
176.12.148.251	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
74.73.231.54	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
157.55.39.138	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
121.216.70.23	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
70.193.208.177	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
141.161.133.216	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.64.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
108.231.154.239	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
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
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
58.172.32.110	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
66.249.64.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
171.98.76.157	Thailand	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.247.36.121	Netherlands	147.237.77.227	e.hamaz.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.64.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.118.11.77	Jordan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
193.178.187.23	Ukraine	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
31.210.186.241	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
82.166.241.113	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
66.249.64.76	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
66.249.64.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
157.55.39.46	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
91.238.134.92	Poland	147.237.8.50	e.tikshuv.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
168.1.75.43	Switzerland	147.237.76.148	gqcenter.aka.idf.i		drop	drop	1
80.230.95.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unexpected post SYN packet - RST or SYN expected	drop	drop	1
184.105.139.123	United States	147.237.0.35	akaws.idf.il		drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	306
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	142
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	133
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	129
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	128
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	15
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	13
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	10
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	9
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	8
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	4
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.47	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.47	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/032204-6.stm	Block	1
216.218.206.66	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.78.34	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.69.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.147	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
171.98.108.245	Thailand	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
66.249.75.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1027-he/atal.aspx	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.229.164.99	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ishurim/exampcert	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17032-he/dover.aspx	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.75.5	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
66.249.79.155	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/tizmoret/news/default.asp	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1065-he/kkkkkkk=f1bab236kkkkkkk_f1bab236	Block	1
66.249.75.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1403-he/atal.aspx	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
46.229.164.113	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/gallery	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20817-he/dover.aspx.	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16789-he/dover.aspx	Block	1
66.249.75.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.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
87.230.26.123	Germany	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	1
180.76.4.179	China	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31//	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
66.249.69.20	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/giyus/www.navy.idf.il	Block	1
66.249.78.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/205-he/patzar.aspx	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/unitfs.asp	Block	1
109.65.54.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
186.166.248.48	Venezuela	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1