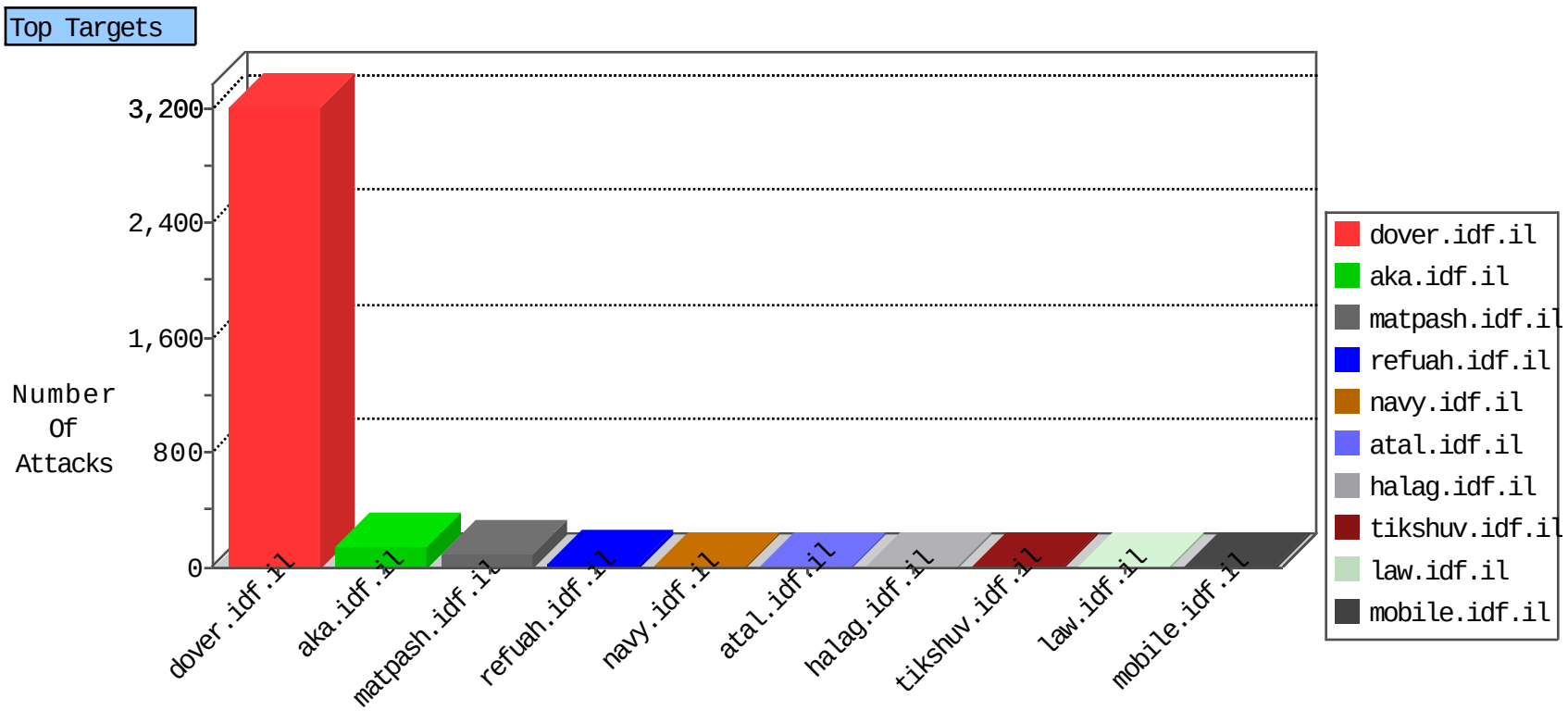
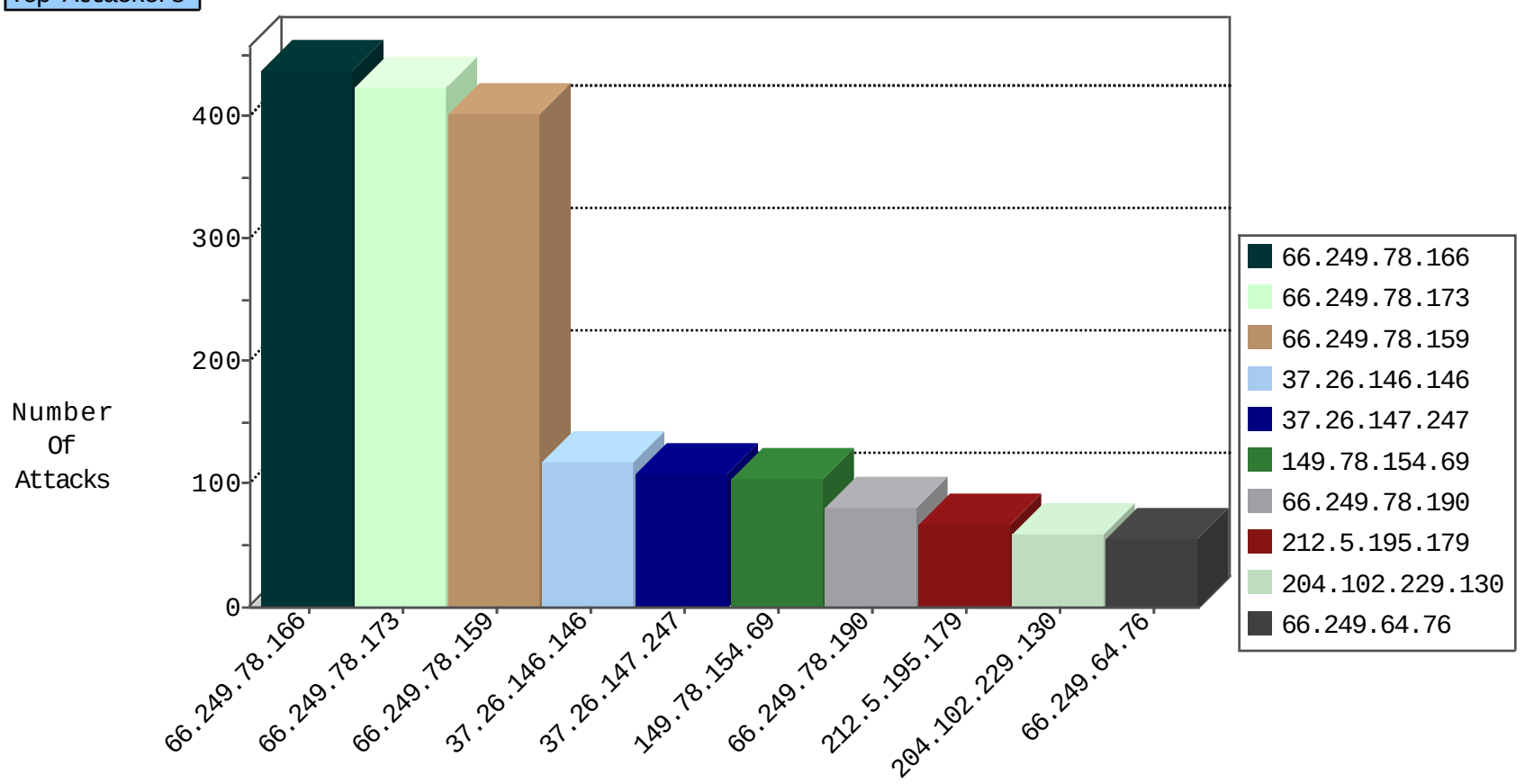
05-01-2015-22:03:02 to 05-01-2015-23:03:02

IDF Under Attack
05-01-2015-22:03:02

Top Targets



Top Attackers



05-01-2015-22:03:02 to 05-01-2015-23:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.173	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	702
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
38.229.1.13	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
61.15.24.148	Hong Kong	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

05-01-2015-22:03:02 to 05-01-2015-23:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.116.202.157	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.25.103.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
93.115.83.16	Anonymous Proxy	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
217.73.129.196	Albania	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
31.210.186.134	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
95.34.26.88	Norway	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
46.210.200.187	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1

05-01-2015-22:03:02 to 05-01-2015-23:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.78.190	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	82
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
2.54.60.170	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.82	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
5.101.157.38	Russian Federation	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
84.228.113.41	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.173	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
23.94.186.178	United States	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
221.229.166.28	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
23.94.186.178	United States	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
109.67.128.52	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
23.94.186.178	United States	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
108.61.193.69	United States	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
23.94.186.178	United States	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
23.94.186.178	United States	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
23.94.186.178	United States	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
23.94.186.178	United States	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
23.94.186.178	United States	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
108.61.193.69	United States	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.64	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
23.94.186.178	United States	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
23.94.186.178	United States	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1

05-01-2015-22:03:02 to 05-01-2015-23:03:02

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.i	First packet isn't SYN	drop	drop	199
66.249.78.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	182
66.249.78.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	161
37.26.146.146	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	119
37.26.147.247	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	109
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	105
212.5.195.179	Slovakia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	67
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	62
204.102.229.130	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
66.249.93.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	49
109.253.130.223	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	44
89.139.41.83	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
12.205.227.2	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	34
93.172.6.255	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
66.249.93.164	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
46.19.86.145	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
46.19.86.247	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
5.101.157.38	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
66.249.64.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
157.55.39.191	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
79.181.164.79	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
66.249.64.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
66.249.64.72	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
31.210.186.134	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
159.26.248.228	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
93.173.140.229	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
66.249.64.76	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
5.28.185.164	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
175.110.76.44	Pakistan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
84.228.113.41	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
80.12.55.254	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
93.168.106.130	Romania	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
46.19.86.67	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
77.125.88.53	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
37.142.7.62	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
207.46.13.8	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
92.241.42.216	Jordan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
109.67.175.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	57
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	55
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	53
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	51
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	51
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	48
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	46
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	44
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	44
46.117.9.195	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 46.117.9.195	Block	42
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	12
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	10
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	9
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	7
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	4
92.113.28.14	Ukraine	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
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	3
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	3
66.249.69.58	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 66.249.69.58	Block	2
185.53.44.85		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//kamlar/printpreview/	Block	2
66.249.78.147	Israel	147.237.0.34	tikshuv.idf.i	Multiple Unauthorized URL Access from 66.249.78.147	Block	2
185.53.44.95		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//chinuch/printpreview/	Block	2
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/search.asp	Block	2
157.55.39.53	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//captcha.ashx	Block	2
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	2
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
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.69.74	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 66.249.69.74	Block	2
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
185.53.44.93		147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/chinuch/miktzoa/	None	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.228.96.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
207.46.13.114	United States	147.237.0.34	tikshuv.idf.i	Multiple Unauthorized URL Access from 207.46.13.114	Block	1
185.53.44.47		147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/patzar/klali/	None	1
185.53.44.121		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//chinuch/printpreview/	Block	1
157.55.39.138	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.138	Block	1
157.55.39.46	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.46	Block	1
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/common/includes/bignewswnd.asp	Block	1
185.53.44.91		147.237.72.166	aka.idf.il	Unknown Parameter catId in aka.idf.il/patzar/home/	None	1
185.53.44.69		147.237.72.166	aka.idf.il	Unknown Parameter CatId in www.aka.idf.il/giyus/qanda/	None	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/independence.stm	Block	1
37.142.7.62	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
178.137.166.68	Ukraine	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
207.46.13.8	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
66.249.75.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1002-he/atal.aspx	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
66.249.69.58	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/trajector/	Block	1