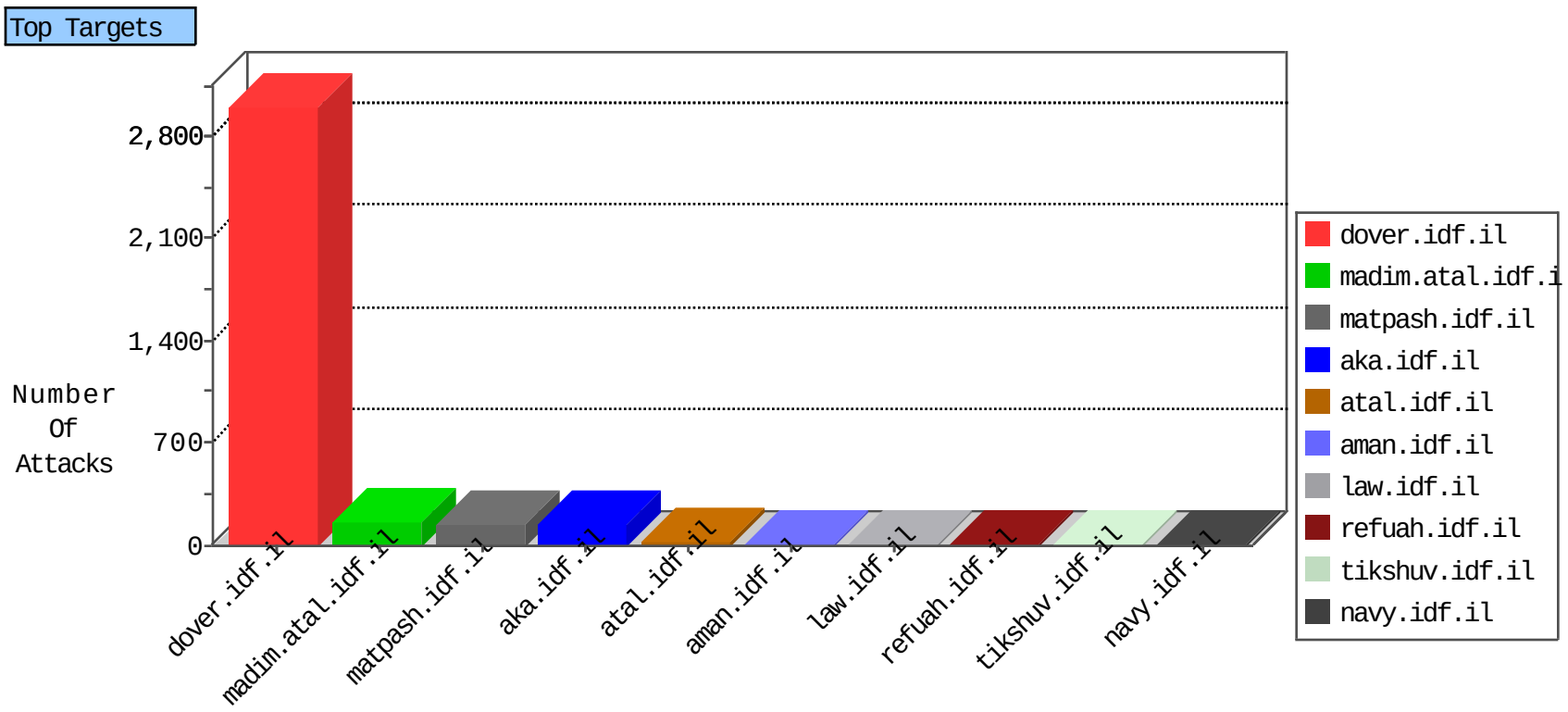
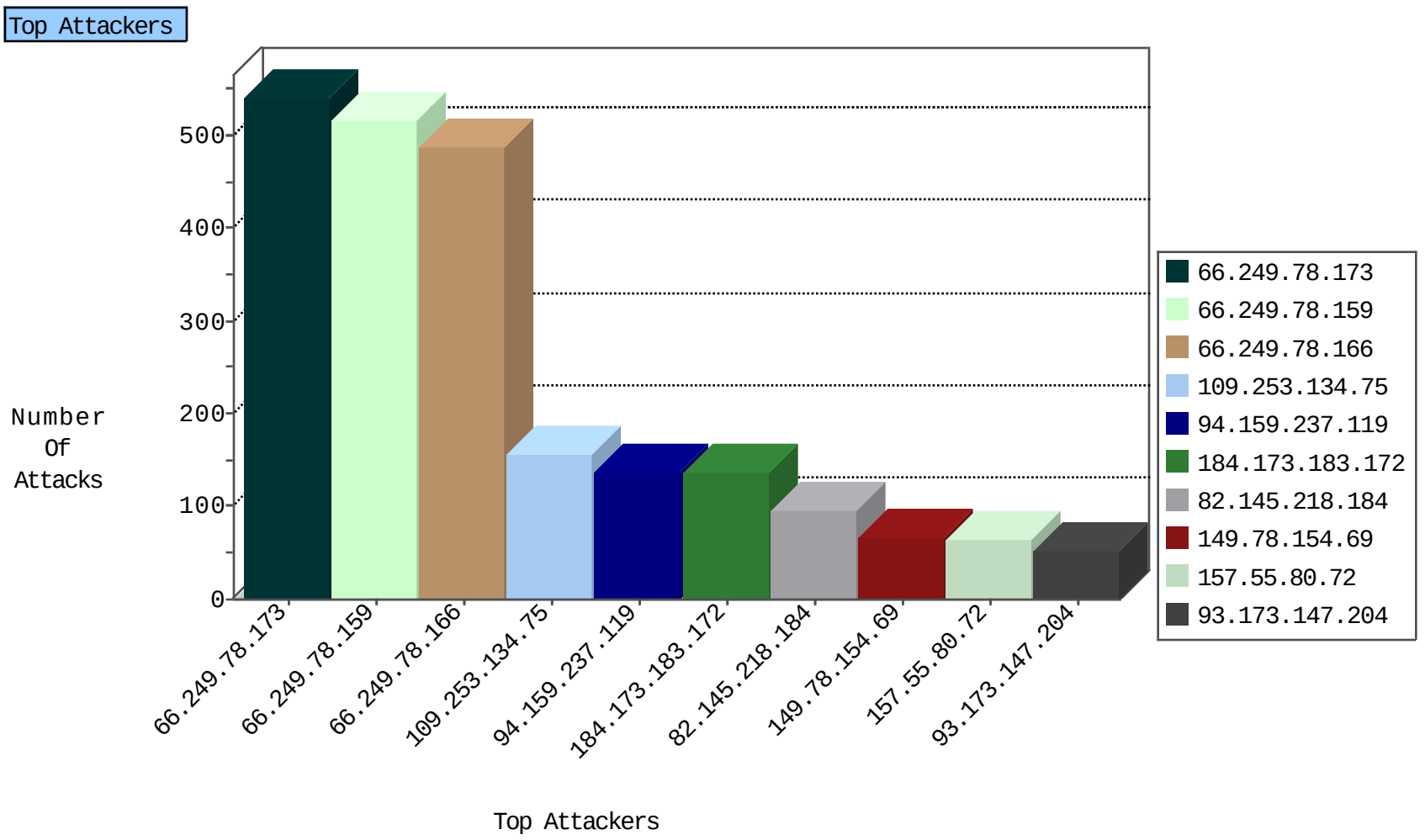
05-01-2015-23:03:06 to 05-02-2015-00:03:06

IDF Under Attack
05-01-2015-23:03:06

Top Targets



Top Attackers



05-01-2015-23:03:06 to 05-02-2015-00:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2928
220.181.108.78	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	610
220.181.108.117	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	170
213.57.46.227	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
84.111.37.49	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
2.54.20.214	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
46.19.85.107	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

05-01-2015-23:03:06 to 05-02-2015-00:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	137
71.6.165.200	United States	147.237.77.233	atal.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
188.138.9.50	Germany	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.216	dover.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
85.25.103.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.44	e.refuah.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
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.27	e.madim.atal.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
188.138.9.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.38	e.e.meitav.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
79.181.208.53	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
23.251.55.233	United States	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1

05-01-2015-23:03:06 to 05-02-2015-00:03:06

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	5
109.65.141.147	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.178.192.198	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
61.240.144.65	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
207.46.13.109	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
23.94.186.178	United States	147.237.76.148	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
23.94.186.178	United States	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
157.55.39.190	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
128.199.75.236	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
89.248.171.167	Netherlands	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
23.94.186.178	United States	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
199.217.118.173	United States	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
23.94.186.178	United States	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
178.32.251.100	France	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
23.94.186.178	United States	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
128.199.165.82	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
110.153.0.142	China	147.237.76.30	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.238.134.92	Poland	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1

05-01-2015-23:03:06 to 05-02-2015-00:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	151
94.159.237.119	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	136
66.249.78.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	136
66.249.78.166	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	115
82.145.218.184	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	96
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	66
157.55.80.72	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	64
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	60
93.173.147.204	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
41.206.130.1	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	44
37.26.148.210	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	43
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
94.163.167.133	Italy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
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
83.76.177.186	Switzerland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	32
192.115.248.2	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
109.160.183.41	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
79.183.174.110	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
41.43.148.247	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
46.19.85.199	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
173.70.19.24	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
188.227.49.254	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
84.228.147.91	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
157.55.39.138	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
193.191.241.1	Belgium	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	15
95.35.50.29	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	15
108.74.24.157	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
79.183.33.93	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
79.182.18.92	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
31.214.27.3	Kuwait	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
77.126.169.182	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
84.133.173.198	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
132.64.43.41	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
46.19.85.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
157.55.39.26	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
109.186.141.128	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
142.22.74.132	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
192.116.175.162	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
188.250.95.86	Portugal	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.134.75	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 109.253.134.75	Block	157
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	130
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	112
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	102
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	100
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	88
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	88
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	86
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	85
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	84
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	14
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	9
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	7
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	7
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	6
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
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	5
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	4
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.197	Block	4
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	4
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_text.asp	Block	3
66.249.79.3	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.79.3	Block	2
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
185.53.44.98		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//kamlar/eurl.axd/85cb72ee4185cb41bf92a8916db47e4d/	Block	2
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.204	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	2
185.53.44.93		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//chinuch/printpreview/	Block	1
23.243.162.193	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/youtub	Block	1
185.53.44.44		147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/kamlar/kishur/	None	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.75.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1442-he/atal.aspx	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
157.55.39.61	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
66.249.69.66	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 66.249.69.66	Block	1
185.53.44.107		147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/chinuch/miktzoa/	None	1
87.68.210.16	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.53.44.70		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//chinuch/printpreview/	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.3	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//captcha.ashx	Block	1
185.53.44.94		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//kamlar/printpreview/	Block	1
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	1
23.251.55.233	United States	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 23.251.55.233	Block	1
185.53.44.53		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//kamlar/eurl.axd/85cb72ee4185cb41bf92a8916db47e4d/	Block	1
66.249.78.125	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/719-4523-he/patzar.aspx	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
87.68.241.175	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
66.249.69.82	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/haredim/webresource.axd	Block	1