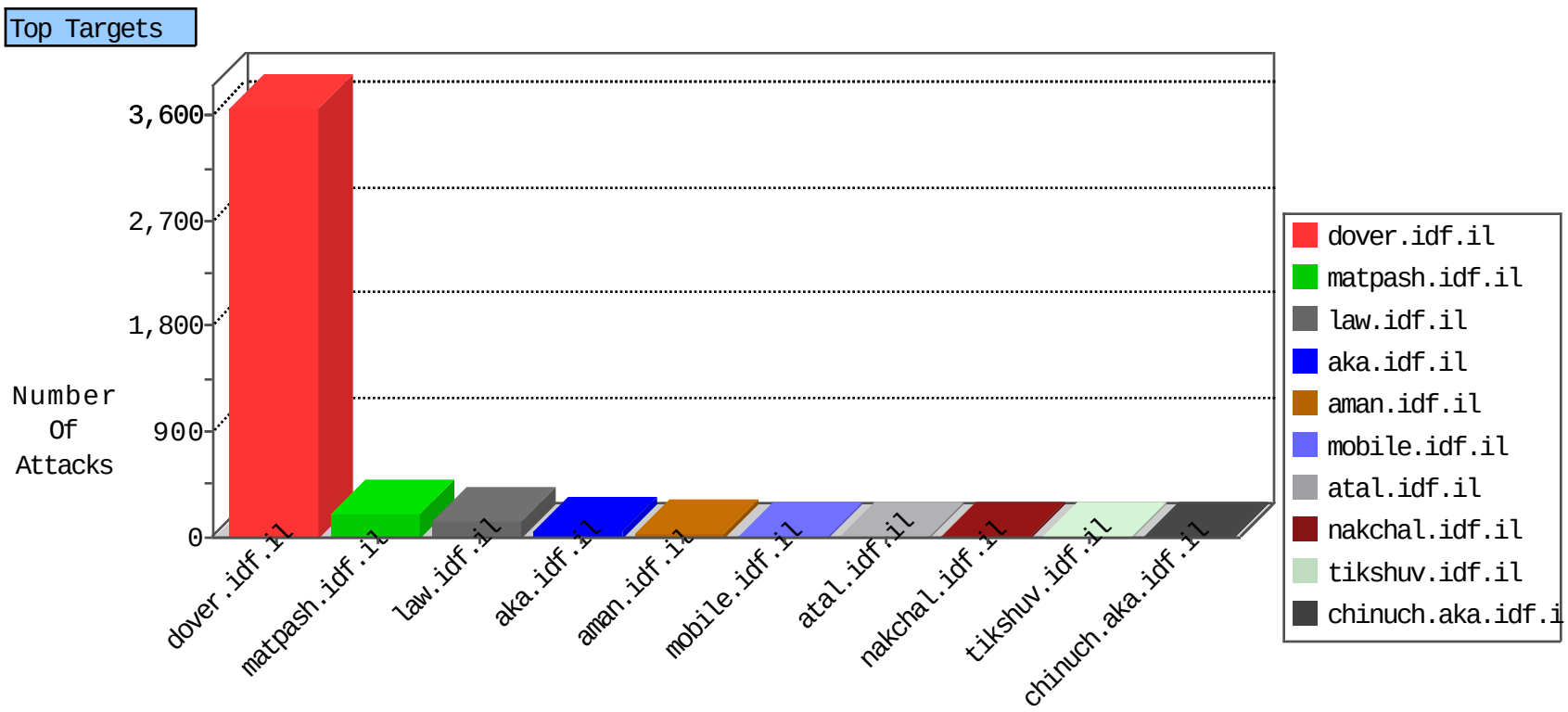
05-02-2015-01:03:02 to 05-02-2015-02:03:02

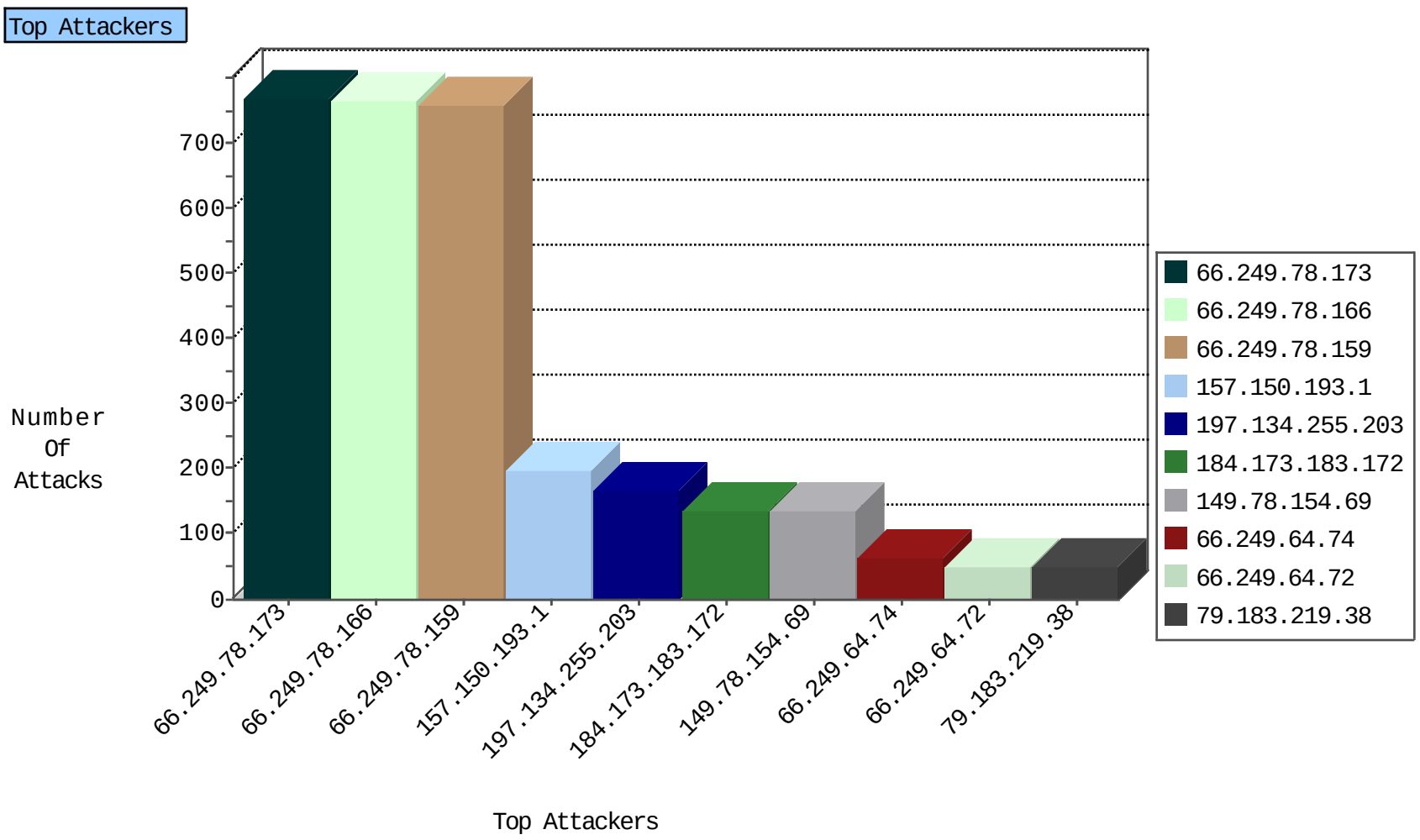
IDF Under Attack
05-02-2015-01:03:02

Top Targets



Top Target

Top Attackers



Top Attackers

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

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	151
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	13
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
146.185.239.100	Russian Federation	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
1.36.191.122	Hong Kong	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

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

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	137
85.25.43.94	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
120.236.0.202	China	147.237.76.30	himush.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
66.240.236.119	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
37.46.39.125	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.178	e.matpash.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

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

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
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.232	United States	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.235	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.139.59.125	Spain	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
2.139.59.125	Spain	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
64.76.71.18	Peru	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
2.139.59.125	Spain	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
60.18.162.244	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
2.139.59.125	Spain	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
175.22.14.71	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
2.139.59.125	Spain	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
2.139.59.125	Spain	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
2.139.59.125	Spain	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
64.76.71.18	Peru	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
2.139.59.125	Spain	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
2.139.59.125	Spain	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
60.18.162.244	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.162	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
221.229.166.28	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.162	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
178.32.251.100	France	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
2.139.59.125	Spain	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
106.39.95.194	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
2.139.59.125	Spain	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1

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

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.il	First packet isn't SYN	drop	drop	189
66.249.78.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	182
197.134.255.203	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	167
157.150.193.1	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	157
66.249.78.159	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	156
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	135
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	70
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	60
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	53
79.183.219.38	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
94.159.137.192	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
84.94.81.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
157.150.193.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	42
50.162.168.246	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
67.21.102.86	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
66.249.64.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
89.139.43.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
166.137.252.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
46.43.89.87	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
188.120.148.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
87.69.241.92	Israel	147.237.72.156	aman.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
69.181.124.57	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
66.249.64.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
66.249.64.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
79.181.22.243	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
62.24.252.133	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
157.55.39.47	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
37.8.122.205	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
84.94.77.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
149.88.112.239	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.80.72	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.138	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
84.228.130.131	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
107.209.18.33	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
188.165.15.195	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
82.145.218.235	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7

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	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	183
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	174
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	172
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	171
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	166
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	155
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	154
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	147
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	140
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.72	Block	27
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.197	Block	15
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	15
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_imgtop.asp	Block	13
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.190	Block	12
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	9
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.76	Block	8
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	8
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.204	Block	7
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	7
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	7
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	5
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
87.69.241.92	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	3
185.53.44.96		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.53.44.96	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
185.53.44.124		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.53.44.124	Block	2
66.249.64.136	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.136	Block	2
66.249.64.75	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//modiin/general	Block	2
66.249.64.75	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/m/	Block	2
185.53.44.85		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.53.44.85	Block	2
66.249.64.76	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/print_text.asp	Block	2
66.249.64.130	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.130	Block	2
185.53.44.80		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.53.44.80	Block	2
66.249.64.73	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/general	Block	1
66.249.75.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
185.53.44.93		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
115.25.81.70	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//aman	Block	1
185.53.44.70		147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 185.53.44.70	Block	1
185.53.44.41		147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//chinuch/printpreview/	Block	1
188.165.15.195	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.213	Israel	147.237.72.156	aman.idf.il	NULL Character in Parameter Value at 19 for www.aman.idf.il/modiin/scripts.asmx/getjs	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.136	Block	1
66.249.78.73	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
185.53.44.96		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arafat/terrorism2/english/main_index.stm	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.53.44.85		147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/chinuch/miktzoa/	None	1
79.181.164.246	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
212.224.119.182	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/golani/golani2.stm	Block	1
185.53.44.44		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/announcements/2002/june/mazen.stm	Block	1
185.53.44.201		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/dayan.stm	Block	1