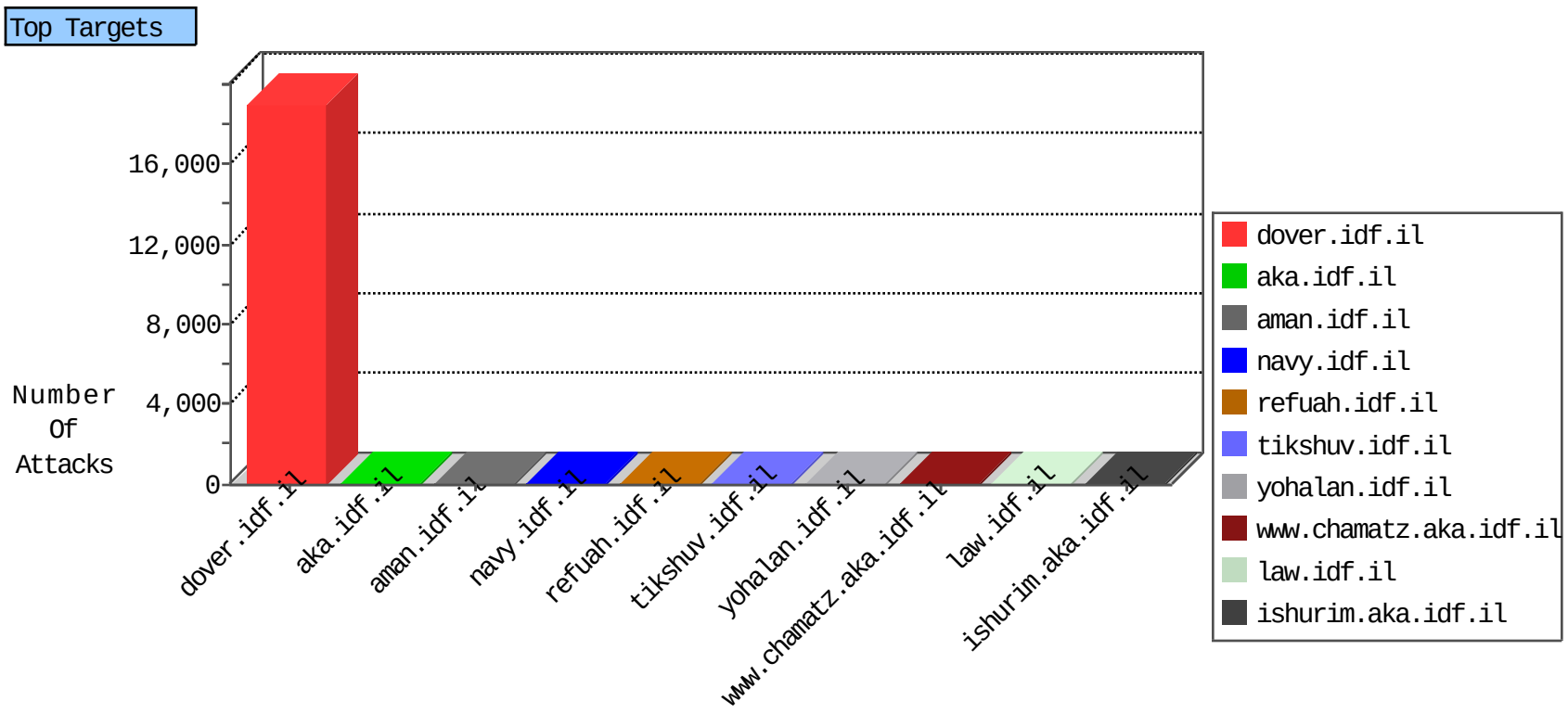
05-02-2015-09:03:01 to 05-02-2015-10:03:01

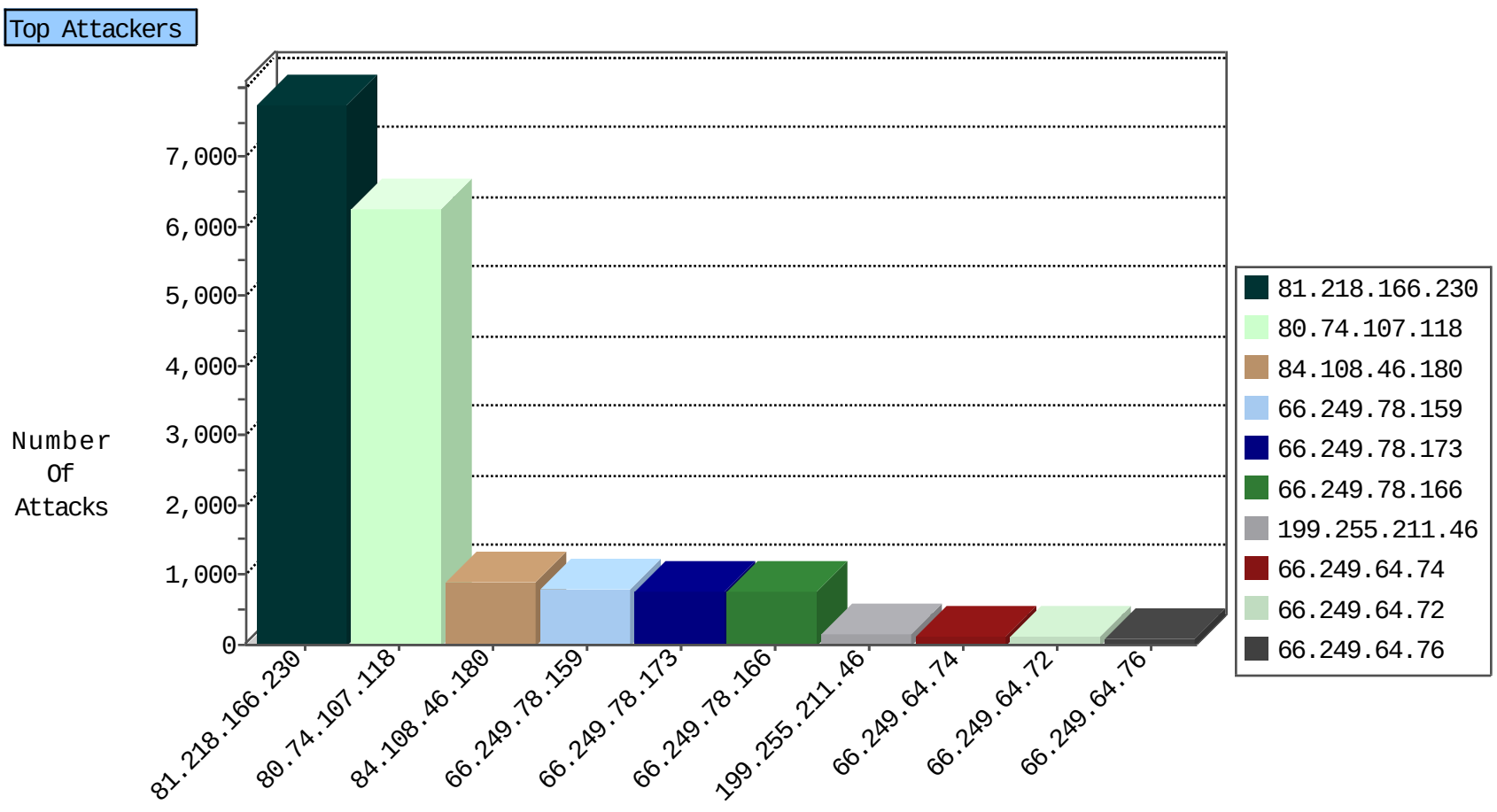
IDF Under Attack
05-02-2015-09:03:01

Top Targets



Top Target

Top Attackers



Top Attackers

05-02-2015-09:03:01 to 05-02-2015-10:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	445
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	293
79.177.171.34	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	233
149.88.104.174	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	110
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
195.37.190.86	Germany	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1

05-02-2015-09:03:01 to 05-02-2015-10:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	22
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.14	e.orchot.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
66.240.192.138	United States	147.237.77.176	matpash.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
79.183.197.33	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
199.168.141.77	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
71.6.167.142	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.216	dover.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
85.25.103.50	Germany	147.237.77.176	matpash.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

05-02-2015-09:03:01 to 05-02-2015-10:03:01

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
87.69.63.177	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.191.161	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.4	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.143.48.200	Korea, Republic of	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
221.143.48.200	Korea, Republic of	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.67	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
218.50.2.105	Korea, Republic of	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
183.232.128.156	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.4	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	Turkey	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.143.48.200	Korea, Republic of	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
218.50.2.105	Korea, Republic of	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
199.168.141.77	United States	147.237.77.216	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	1
43.255.191.161	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
183.232.128.156	China	147.237.77.235	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.161	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.4	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1

05-02-2015-09:03:01 to 05-02-2015-10:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
81.218.166.230	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7764
80.74.107.118	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6255
84.108.46.180	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	906
66.249.78.159	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	512
66.249.78.166	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	501
66.249.78.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	500
199.255.211.46	Anonymous Proxy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	147
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	109
66.249.78.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	102
66.249.78.166	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	96
66.249.64.74	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	72
66.249.64.72	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	61
66.249.64.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	59
46.19.86.93	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
79.176.198.243	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	40
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
66.249.64.72	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
66.249.64.74	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	25
85.65.14.139	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.64.76	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
157.55.39.191	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
157.55.39.47	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
81.218.251.252	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
41.129.70.203	Egypt	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
66.249.93.164	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
66.249.93.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
77.42.157.194	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
37.26.148.197	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
36.252.154.104	Nepal	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
157.55.39.136	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
149.88.11.194	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
66.249.93.160	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
84.228.10.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
103.15.246.181	Bangladesh	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
46.117.252.100	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
79.181.152.94	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11

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	131
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	114
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	99
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	42
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	34
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	19
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	16
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	Multiple Unauthorized URL Access from 66.249.64.76	Block	9
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
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/view_img.asp	Block	6
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	5
85.250.73.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	3
37.26.148.197	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
37.26.148.197	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.26.148.197	Block	2
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
212.143.136.114	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mce_src=	Block	2
207.46.13.101	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.101	Block	2
5.102.241.36	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
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	2
207.46.13.109	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.46.13.109	Block	2
85.65.14.139	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	2
188.165.15.195	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.195	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18858-he/dover.aspx	Block	1
85.250.24.69	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/relativecontact.aspx	None	1
66.249.75.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	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
109.67.154.30	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.200.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il//sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0402-1.stm	Block	1
188.165.15.195	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arafat/terrorism/english/main_index.stm	Block	1
66.249.78.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/261-6662-he/patzar.aspx	Block	1
66.249.64.159	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.136	Block	1
37.26.148.197	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyius	Block	1
85.250.49.186	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.113	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/m/	Block	1
149.78.107.141	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.67.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/brothers	Block	1
54.80.111.147	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.101	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/hovot/templates/main.asp	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0925-2.stm	Block	1
66.249.78.45	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/894-ar	Block	1
149.78.107.141	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/announcements/2002/june/poland/poland.stm	Block	1