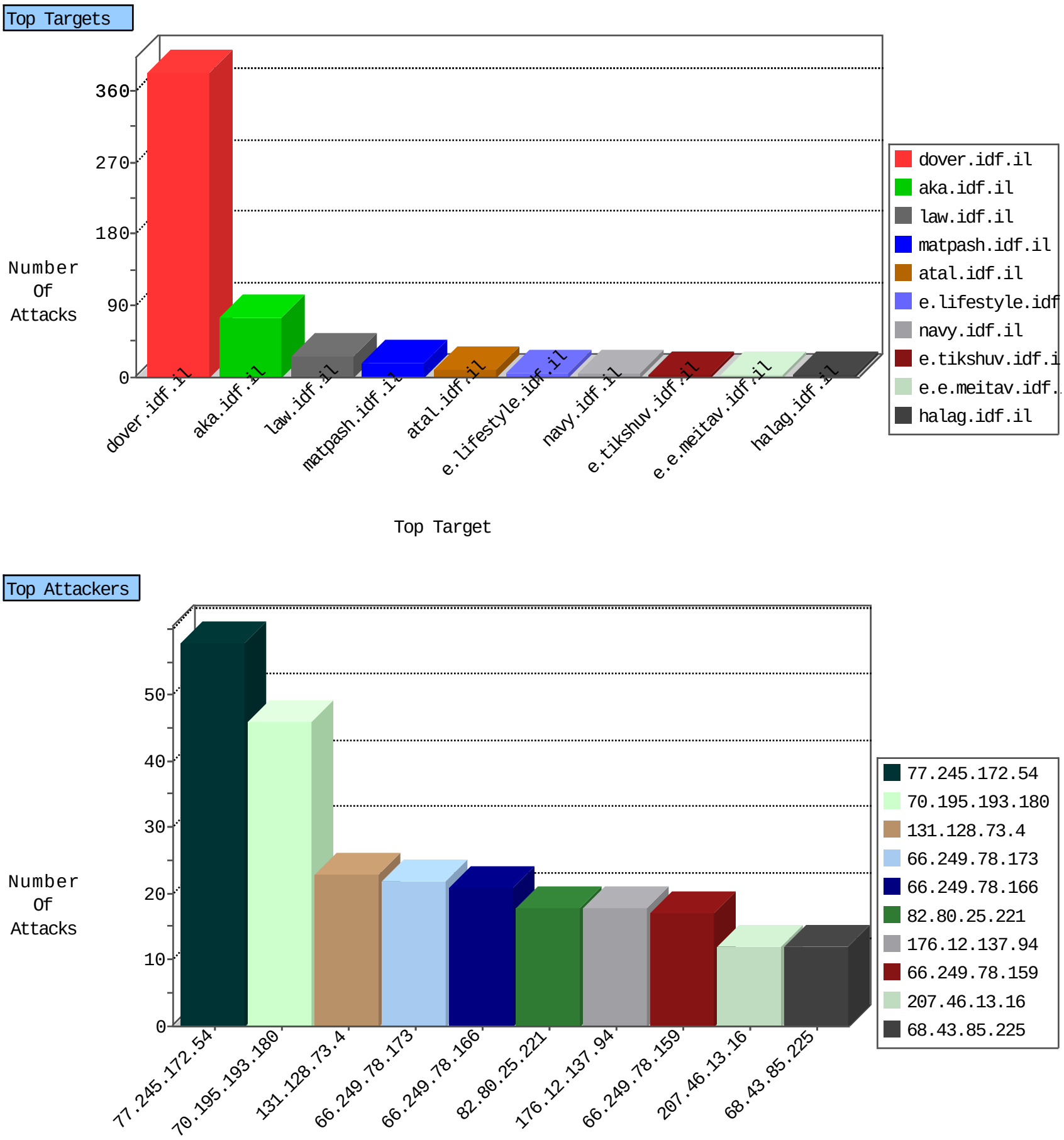
03-30-2015-05:03:07 to 03-30-2015-06:03:07

IDF Under Attack
03-30-2015-05:03:07



03-30-2015-05:03:07 to 03-30-2015-06:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.42	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	957
68.43.85.225	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	12
24.188.18.191	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	11
174.236.132.3	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	8
207.46.13.16	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	7
203.192.89.50	Australia	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	6
66.108.203.40	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	6
66.249.78.166	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	6
66.249.78.173	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	6
108.48.14.174	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	6
131.128.73.4	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
5.255.253.99	Russian Federation	147.237.77.74	law.idf.il	unblock-sp-traf1	forward	5
157.55.39.42	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
207.46.13.112	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
99.180.77.33	United States	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
157.55.39.6	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
50.46.114.19	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
207.46.13.5	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	4
77.245.172.54	Russian Federation	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
66.249.78.159	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
157.55.39.41	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
188.165.15.148	France	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
24.96.87.140	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
204.237.22.235	Canada	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
157.55.39.67	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	3
203.147.10.65	Thailand	147.237.76.38	e.e.meitav.idf.il	L4 Source or Dest Port Zero	drop	3
157.55.39.153	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
24.90.111.185	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
66.249.78.89	United States	147.237.77.74	law.idf.il	unblock-sp-traf1	forward	2
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
66.249.78.160	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	2
190.18.50.16	Argentina	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	2
173.199.65.52	Canada	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
136.243.36.97	Germany	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
188.165.15.22	France	147.237.77.234	halag.idf.il	unblock-sp-traf1	forward	2
66.249.78.22	United States	147.237.77.74	law.idf.il	unblock-sp-traf1	forward	2
54.72.73.168	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
50.67.161.250	Canada	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
65.55.210.133	United States	147.237.77.233	atal.idf.il	unblock-sp-traf1	forward	2
91.108.74.105	Germany	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
66.249.81.212	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	1
172.56.29.26	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	1
157.55.39.125	United States	147.237.77.170	maarachot.idf.il	unblock-sp-traf1	forward	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	1
69.35.216.60	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	1
199.30.24.46	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1

03-30-2015-05:03:07 to 03-30-2015-06:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count

03-30-2015-05:03:07 to 03-30-2015-06:03:07

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	18
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
218.77.79.43	China	147.237.77.243	mobile.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
74.87.109.45	United States	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
212.147.56.190	Switzerland	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.67	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
212.147.56.190	Switzerland	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.66	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.7	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
146.148.116.230		147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.141	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
117.40.240.221	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
117.40.240.221	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
117.40.240.221	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
218.6.132.45	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
212.147.56.190	Switzerland	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
146.148.116.230		147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.141	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
146.148.116.230		147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.141	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
117.40.240.221	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
117.40.240.221	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1

03-30-2015-05:03:07 to 03-30-2015-06:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
77.245.172.54	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	54
70.195.193.180	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	19
70.195.193.180	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	19
131.128.73.4	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
176.12.137.94	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
46.19.86.114	Israel	147.237.77.74	law.idf.il	Invalid ACK number	Bad TCP sequence	monitor	10
70.195.193.180	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	8
176.12.144.82	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.64.150	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.142.195	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
109.253.157.32	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
176.12.146.76	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
85.130.228.108	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
109.253.156.187	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
69.171.237.115	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	4
69.171.237.116	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.6	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
69.171.237.113	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	2
207.241.229.147	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
141.212.122.40	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
41.189.35.248	Cote D'Ivoire	147.237.77.176	matpash.idf.il	header rejection pattern found in request	Header Rejection	monitor	1
218.22.211.69	China	147.237.8.24	e.lifestyle.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.40	United States	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
79.176.41.191	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.19.85.91	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
79.176.41.191	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.36	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
170.140.105.65	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
178.32.128.216	France	147.237.77.74	law.idf.il	ICQ Connection over HTTP detected	Instant Messengers	monitor	1
141.212.122.38	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
207.46.13.16	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.16	Block	4
157.55.39.6	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	4
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	3
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
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
77.126.250.88	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
178.32.128.216	France	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 178.32.128.216	Block	2
157.55.39.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.42	Block	2
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	Block	2
66.249.78.102	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
176.12.146.215	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.41	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1217-5.stm	Block	1
2.54.174.239	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
85.250.82.218	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	1
176.12.143.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.121.114.7	Israel	147.237.72.166	aka.idf.il	Unknown Parameter _ in www.aka.idf.il/main/sachar/home.aspx	None	1
109.253.146.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.159	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2001/february/14.stm	Block	1
87.68.9.188	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
66.249.78.213	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.143.120	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
54.163.105.38	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1124-1.stm	Block	1
109.253.156.187	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.30.187	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/home.aspx	None	1
66.249.78.160	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
178.32.128.216	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/news/imgoff	Block	1
37.26.146.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
89.138.69.223	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/february/06.stm	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.75.58	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on 147.237.76.86//scriptresource.axd	Block	1
176.12.146.119	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.157.32	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.250.30.187	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$rbSearchSites in aka.idf.il/main/sachar/	None	1
66.249.78.160	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim1/templates/main.asp	Block	1
181.90.20.117	Argentina	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
176.12.139.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
41.189.35.248	Cote D'Ivoire	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	1
109.253.135.181	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/093.stm	Block	1
66.249.75.74	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/scriptresource.axd	Block	1
176.12.146.119	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __EVENTTARGET in aka.idf.il/main/sachar/	None	1
85.250.82.218	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
188.165.15.121	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1403-he/atal.aspx	Block	1
176.12.142.195	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
41.189.35.248	Cote D'Ivoire	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1
109.253.137.183	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1