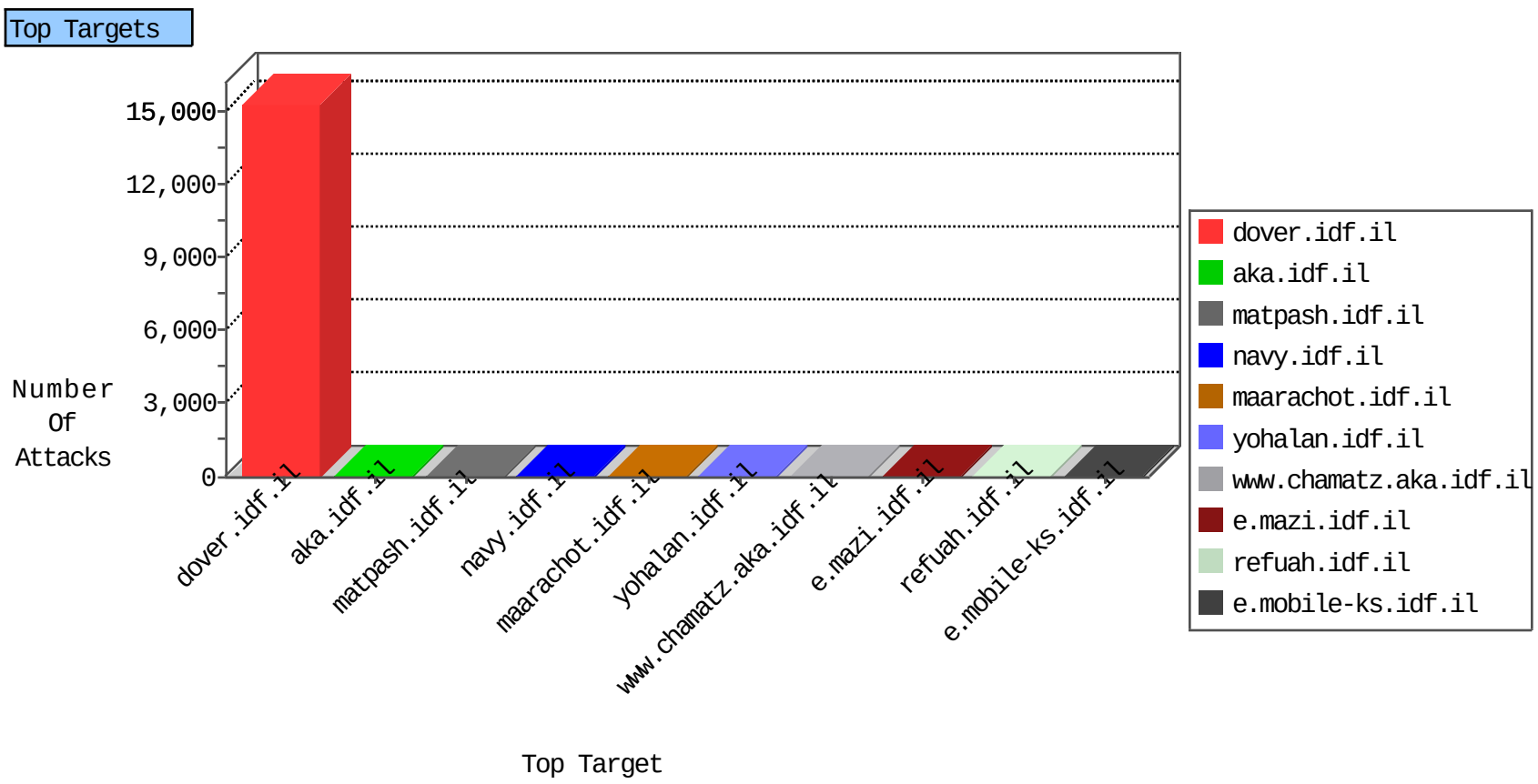
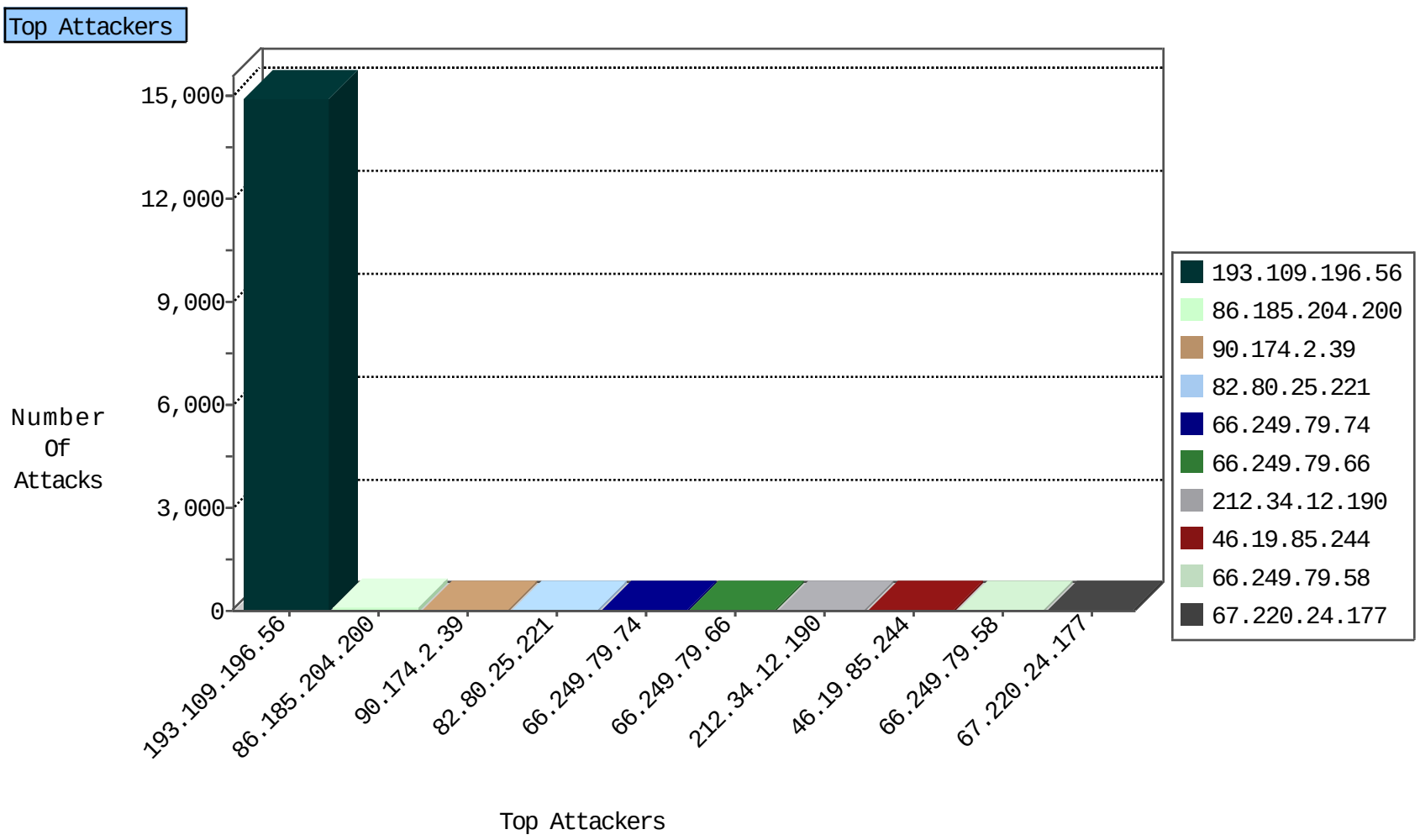
03-27-2015-01:03:02 to 03-27-2015-03:03:02

IDF Under Attack
03-27-2015-01:03:02

Top Targets



Top Attackers



03-27-2015-01:03:02 to 03-27-2015-03:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
86.185.204.200	United Kingdom	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	73
212.34.12.190	Jordan	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	16
67.220.24.177	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	12
95.45.168.47	Ireland	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	10
68.58.211.148	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	8
91.66.162.61	Germany	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	7
96.50.248.143	Canada	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	7
75.89.194.194	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	7
69.254.193.10	United States	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	7
86.42.58.193	Ireland	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	6
188.165.15.148	France	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	6
99.237.226.211	Canada	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	6
5.67.63.248	United Kingdom	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
74.120.99.138	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
207.46.13.5	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	5
208.99.166.94	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
24.60.201.204	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	5
67.86.2.60	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	4
157.55.39.67	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	3
50.87.144.145	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	3
157.55.39.137	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	3
69.254.193.10	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
204.237.22.235	Canada	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
207.190.221.195	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
157.55.39.99	United States	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	2
5.255.253.16	Russian Federation	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	2
157.55.39.6	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
66.249.73.132	United States	147.237.72.166	aka.idf.il	unblock-sp-traf1	forward	2
125.175.81.14	Japan	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	2
5.255.253.99	Russian Federation	147.237.77.74	law.idf.il	unblock-sp-traf1	forward	2
86.197.18.140	France	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	2
74.95.70.221	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
178.175.139.142	Moldova, Republic of	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	1
66.249.67.1	United States	147.237.0.15	kosher-kravi.idf.il	unblock-sp-traf1	forward	1
217.69.133.14	Russian Federation	147.237.77.74	law.idf.il	unblock-sp-traf1	forward	1
74.95.70.221	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
162.212.1.172	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
138.130.236.90	Australia	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
93.158.143.28	Russian Federation	147.237.77.170	maarachot.idf.il	unblock-sp-traf1	forward	1
71.6.135.131	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	unblock-sp-traf1	forward	1
217.69.133.67	Russian Federation	147.237.77.176	matpash.idf.il	unblock-sp-traf1	forward	1
74.95.70.221	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
162.243.210.161	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
54.72.0.55	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
190.115.26.26	Belize	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1
74.95.70.221	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
74.95.70.221	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	unblock-sp-traf1	forward	1

03-27-2015-01:03:02 to 03-27-2015-03:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
212.34.12.190	Jordan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	6
175.44.25.203	China	147.237.76.42	refuah.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	2
18.239.0.155	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
96.50.248.143	Canada	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
207.201.223.195	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1

03-27-2015-01:03:02 to 03-27-2015-03:03:02

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	31
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
218.205.231.189	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
218.205.231.189	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
98.143.148.47	United States	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
218.205.231.189	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
187.32.92.225	Brazil	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
187.32.92.225	Brazil	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
141.255.190.190	Sweden	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.205.231.189	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
130.211.149.193		147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
218.205.231.189	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
113.59.33.61	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 4096	1
218.205.231.189	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
101.226.179.84	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.205.231.189	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
82.165.143.210	Germany	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.205.231.189	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
187.32.92.225	Brazil	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
187.32.92.225	Brazil	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
222.69.94.13	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.161	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
187.32.92.225	Brazil	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.205.231.189	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
130.211.149.193		147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
218.205.231.189	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
130.211.149.193		147.237.76.34	yohalan.idf.il	ET SCAN NMAP -f -sS	1

03-27-2015-01:03:02 to 03-27-2015-03:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
90.174.2.39	Spain	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	36
66.249.79.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
66.249.79.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
46.19.85.244	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.79.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
46.19.85.46	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
37.247.36.98	Netherlands	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
79.178.152.166	Israel	147.237.77.226	www.chamatz.aka.idf.il	First packet isn't SYN	drop	drop	3
164.138.125.57	Israel	147.237.77.216	dover.idf.il	Web Servers Slow HTTP Denial of Service	Web Server Enforcement Violation	reject	2
41.44.209.208	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
2.54.36.196	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
2.54.36.196	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
188.138.17.205	France	147.237.77.121	e.navy.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
31.210.186.153	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.162	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
80.246.137.134	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

03-27-2015-01:03:02 to 03-27-2015-03:03:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
193.109.196.56	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to hss/	Block	14935
213.251.182.10	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	6
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
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	2
52.4.32.145	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
109.253.128.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.79.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/december/30a.stm	Block	1
217.69.133.224	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/afhyrim	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	1
164.138.125.57	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 164.138.125.57	Block	1
54.158.186.118	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
115.25.81.74	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.79.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	1
37.142.205.169	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 37.142.205.169	Block	1
164.138.125.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
79.177.158.39	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.58	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/scriptresource.axd	Block	1
207.46.13.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-15582-he/dover.aspx	Block	1
138.130.236.90	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il./	Block	1
66.249.79.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2001/november/6.stm	Block	1
52.0.69.200	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
176.12.148.15	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
94.159.132.3	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
66.249.67.58	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/webresource.axd	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	Block	1
164.138.125.57	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
66.249.79.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.stm	Block	1
52.1.4.57	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
101.226.179.84	China	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
66.249.67.66	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on 147.237.76.86//scriptresource.axd	Block	1
164.138.125.57	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
66.249.79.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1

03-27-2015-01:03:02 to 03-27-2015-03:03:02