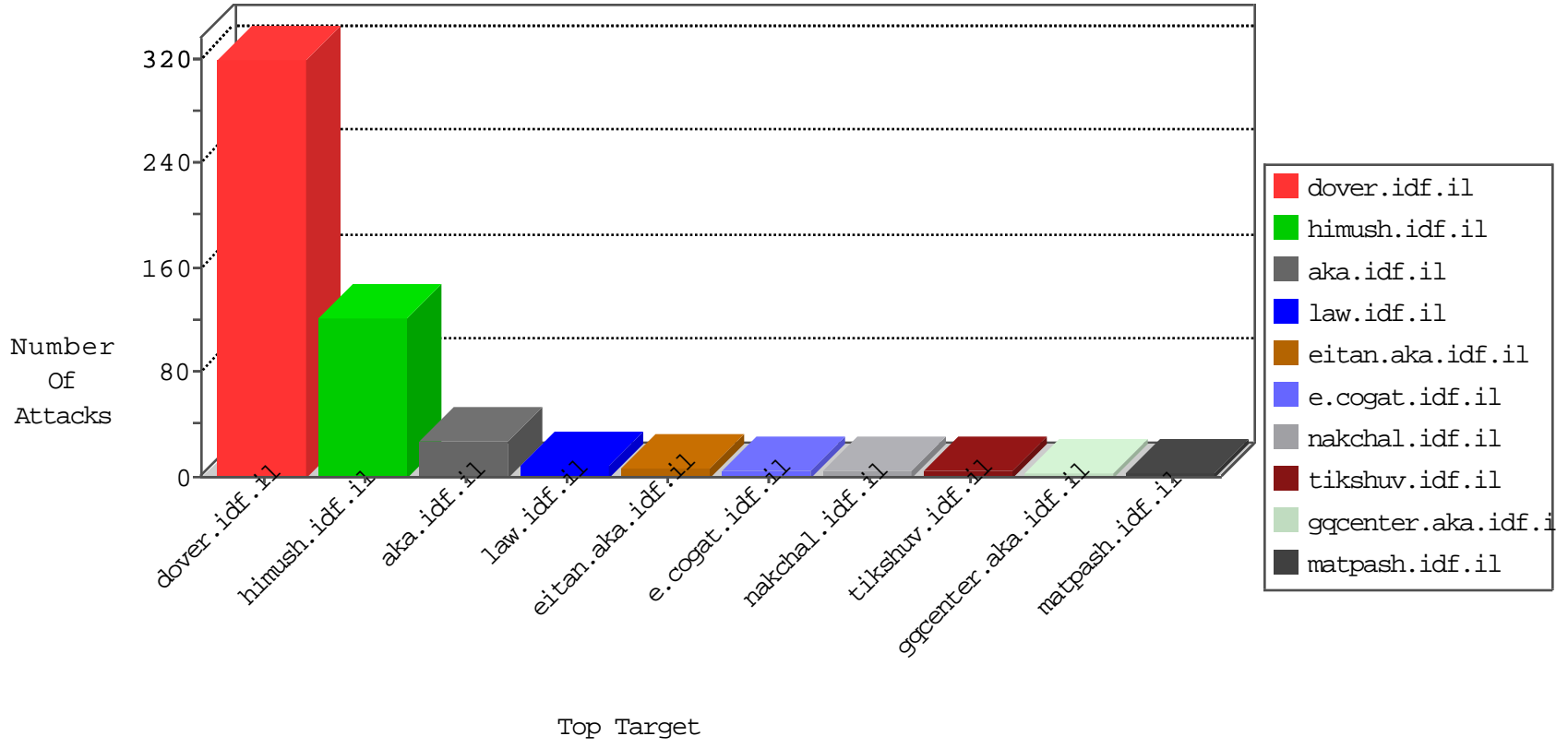
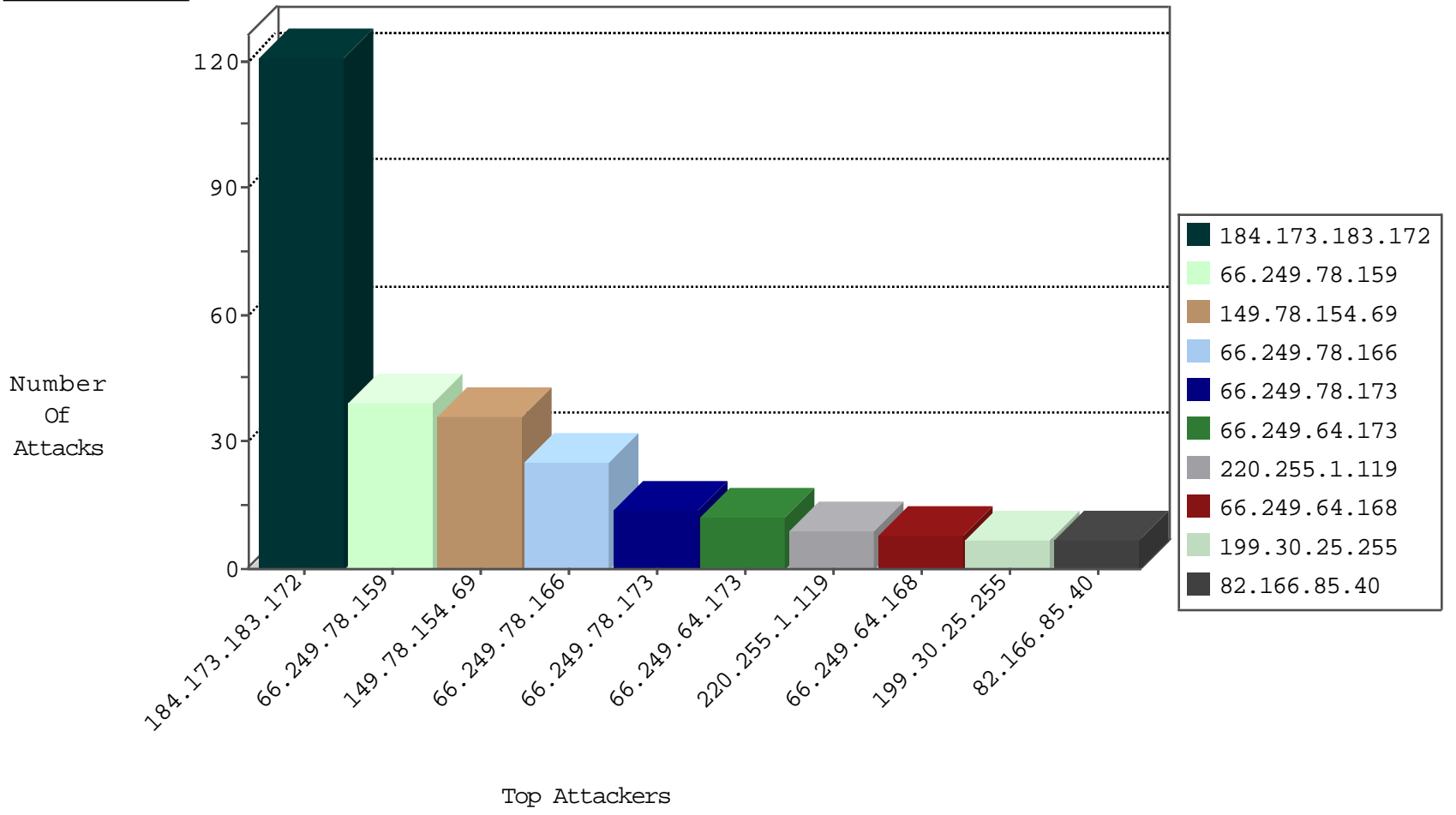




Top Targets



Top Attackers



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	76
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	52
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
192.3.207.66	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
188.138.9.50	Germany	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
192.3.207.66	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.76.30	himush.idf.il	DVRep_P-N_40-59	Permit	121
46.116.210.130	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.34	tikshuv.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
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
109.201.154.140	Netherlands	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.16	my-kosher-kravi.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	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.233	atal.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

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
24.155.160.204	United States	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
163.13.118.99	Taiwan	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
121.88.5.177	Korea, Republic of	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
89.248.160.215	Netherlands	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	China	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
211.149.240.162	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
203.113.9.143	Thailand	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
60.169.78.79	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
203.113.9.143	Thailand	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
24.155.160.204	United States	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
188.138.9.51	Germany	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
24.155.160.204	United States	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
163.13.118.99	Taiwan	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
121.88.5.177	Korea, Republic of	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
211.149.240.162	China	147.237.77.234	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.65	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
203.113.9.143	Thailand	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.64	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
203.113.9.143	Thailand	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	1
60.18.162.244	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	38
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
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
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
66.249.64.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
220.255.1.119	Singapore	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
66.249.64.168	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
82.166.85.40	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
77.127.212.122	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
41.42.175.230	Egypt	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
41.42.152.41	Egypt	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
220.255.1.149	Singapore	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
173.167.5.121	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
173.78.15.103	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
68.180.229.51	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
157.55.39.6	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
46.19.85.40	Israel	147.237.77.74	law.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
149.78.240.88	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
220.255.1.167	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
157.55.39.204	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
220.255.1.111	Singapore	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
24.114.70.131	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
118.241.234.224	Japan	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
41.42.160.65	Egypt	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
199.30.25.255	United States	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	2
220.255.1.128	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
203.127.96.237	Singapore	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
157.55.39.162	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
220.255.1.101	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
66.249.64.178	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
220.255.1.131	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
203.127.96.246	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
41.233.165.1	Egypt	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
220.255.1.102	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
199.30.25.255	United States	147.237.77.216	dover.idf.i	Unexpected post SYN packet - RST or SYN expected	drop	drop	2
220.255.1.132	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
220.255.1.110	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
69.248.82.82	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
220.255.1.146	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
2.54.28.34	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
220.255.1.103	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
203.127.58.231	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
157.55.39.7	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
199.30.25.255	United States	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	2
220.255.1.121	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
157.55.39.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.66	Block	2
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
199.30.25.93	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.111	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/164-5106-he/patzar.aspx	Block	1
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16054-en/dover.asp	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/idf_in_pictures/kkkkkkk=d6585104kkkkkkk_d6585104	Block	1
79.178.53.133	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.130	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_text.asp	Block	1
66.249.67.65	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71519-he/maarachot.aspx	Block	1
180.76.5.61	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/1043-7713-he/cogat.aspx	Block	1
85.65.165.181	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.82	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.229.51	Block	1
66.249.67.88	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/938-he/nakhal.aspx	Block	1
188.165.15.117	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim	Block	1
92.226.50.43	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16893-he/dover.aspx	Block	1
46.19.85.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/library/manage/resource/getfilecontent.hh.asp	Block	1
74.82.47.3	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.67.105	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/261-6616-he/patzar.aspx	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
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-14478-he/dover.aspx	Block	1
66.199.231.242	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
77.237.146.28	Czech Republic	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1