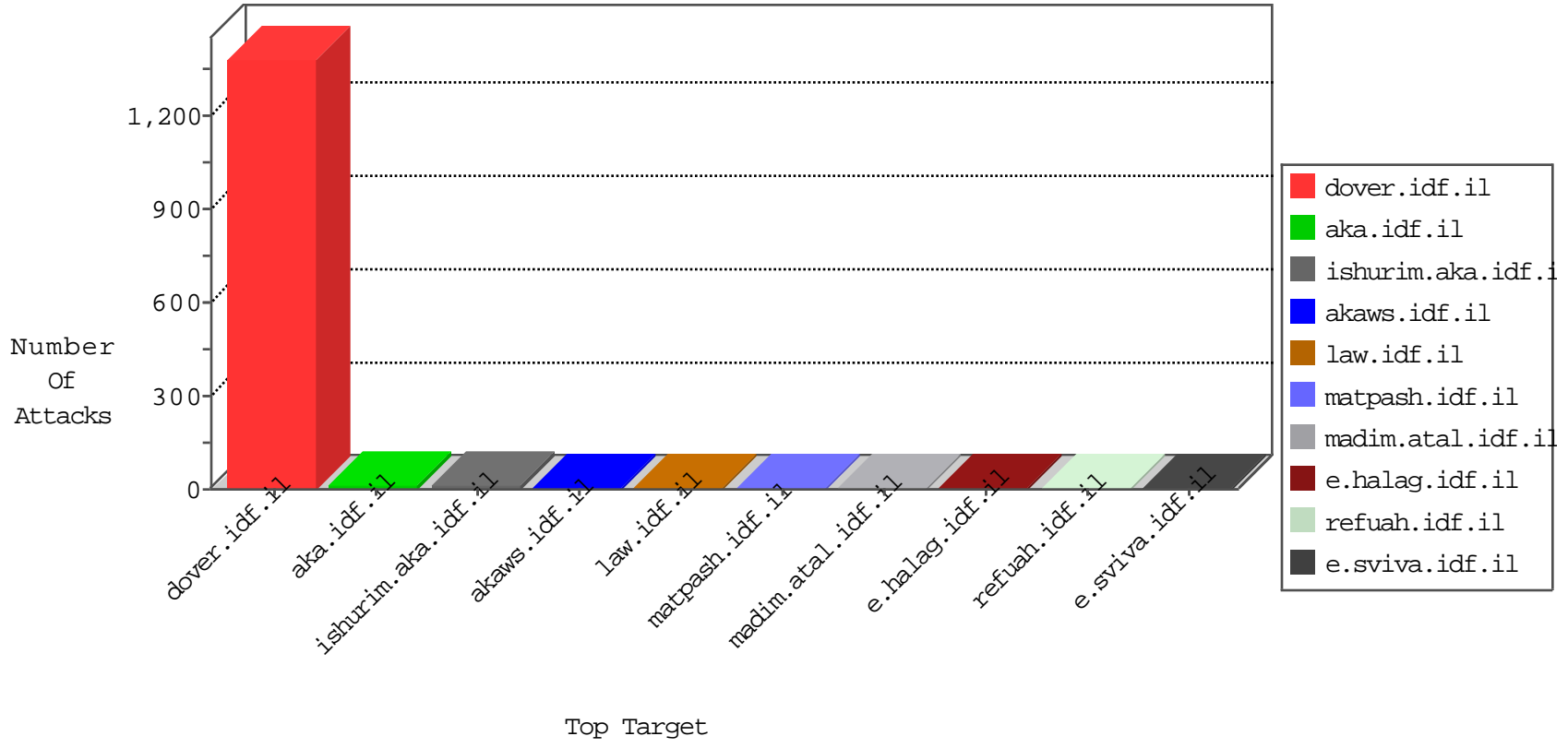
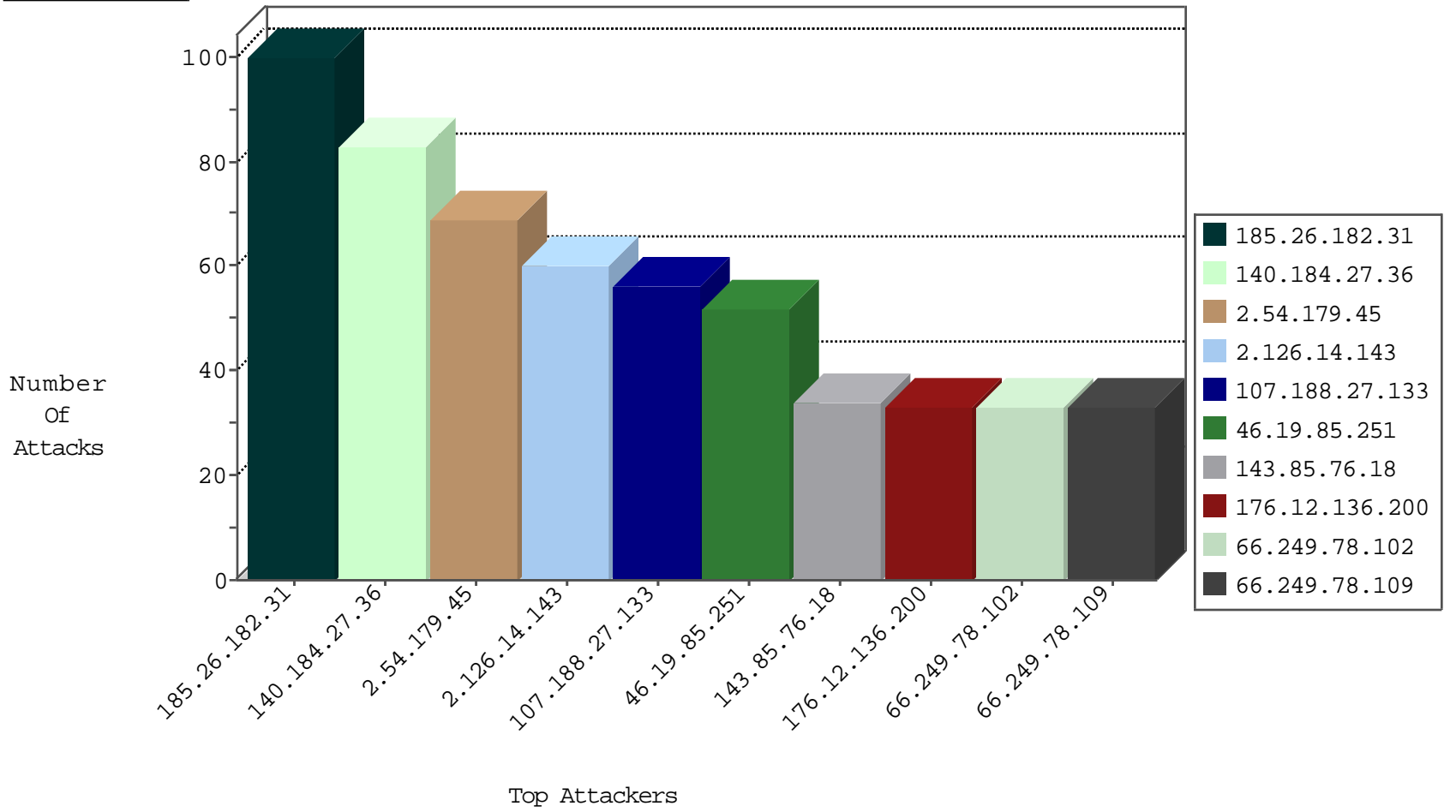




Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.64.2	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	871
220.181.108.171	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	377
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	90
220.181.108.79	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	33
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.167.142	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	2
85.25.103.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.147	chimuch.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.147	chimuch.aka.idf.il	DVRep_B-N_60_100	Block	1
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1
71.6.165.200	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
84.228.180.200	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.77.216	dover.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
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	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
5.63.150.76	United Kingdom	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	1
198.20.70.114	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.31	nakchal.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
71.6.135.131	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.46	e.chimuch.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	5
113.57.151.37	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
111.203.22.56	China	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
111.1.51.42	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
221.235.205.123	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
111.1.51.42	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
199.116.250.199	United States	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.176	matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
194.63.140.245	Russian Federation	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.76.148	ggcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
187.11.121.110	Brazil	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
119.181.119.15	China	147.237.0.33	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
61.240.144.65	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
113.57.151.37	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
61.149.161.186	China	147.237.76.196	e.sviva.idf.il	GPL SCAN nmap TCP	1
113.57.151.37	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -f -sS	1
111.1.51.42	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
111.1.51.42	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
221.235.205.123	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
111.1.51.42	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
187.11.121.110	Brazil	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.67	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
178.19.107.114	Poland	147.237.76.30	hinush.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential VNC Scan 5800-5820	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
185.26.182.31	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	100
140.184.27.36	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	83
2.54.179.45	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	69
2.126.14.143	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	60
46.19.85.251	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
107.188.27.133		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
143.85.76.18	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
176.12.136.200	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
2.54.184.20	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
207.46.13.95	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
2.52.58.16	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
73.15.124.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
66.249.78.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
17.142.152.86	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
200.18.49.10	Brazil	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
207.46.13.52	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
174.253.192.178	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
17.142.152.111	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
17.142.151.234	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
188.120.148.195	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	12
176.12.141.125	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
17.142.152.110	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
17.142.152.81	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
66.249.78.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
107.188.27.133		147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	11
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
76.99.230.140	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
201.227.226.145	Panama	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
201.227.226.150	Panama	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
207.46.13.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
17.142.145.3	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
62.210.189.96	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
66.249.78.109	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
17.142.152.72	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
220.255.1.153	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
66.249.78.109	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	7
77.125.119.104	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
98.113.166.238	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
173.74.110.162	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
66.249.78.95	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	6
79.179.179.188	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
107.4.124.185	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.251.182.103	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	3
157.55.39.5	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
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
157.55.39.178	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.178	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1226-he/refuah.aspx	Block	1
66.249.64.71	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71652-he/maarachot.aspx	Block	1
194.187.168.20	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/givati/	Block	1
150.242.219.5		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
216.244.83.168	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/html/10.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/0119-3.stm	Block	1
66.249.64.73	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71868-he/maarachot.aspx	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13606-he/dover.aspxx³Ã- x³Ã?x³Ö³Ã-Ö²Ã¿Ö²Ã¿	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-he/dover.aspx	Block	1
173.208.203.138	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.69.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
207.46.13.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1116-he/x x"	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/home.asp/news.asp	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
66.249.64.24	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-17592-en/dover.aspx	Block	1
180.76.4.211	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
87.68.86.103	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/pirsunemofet.aspx	None	1
66.249.69.36	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
212.199.136.107	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakchal.idf.il/page.asp	Block	1
157.55.39.24	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13437-he/dover.aspxx³Ö³Ã-Ö²Ã¿Ö²Ã¿x³Ã?x³Ö³Ã-Ö²Ã¿Ö²Ã¿x³Ö³Ã-Ö²Ã¿Ö²Ã¿x³Ãf	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
66.249.64.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-16800-en/dover.aspx	Block	1
188.165.15.13	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info03.stm	Block	1
142.54.161.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11306-en/dover.aspx/trackback/	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1