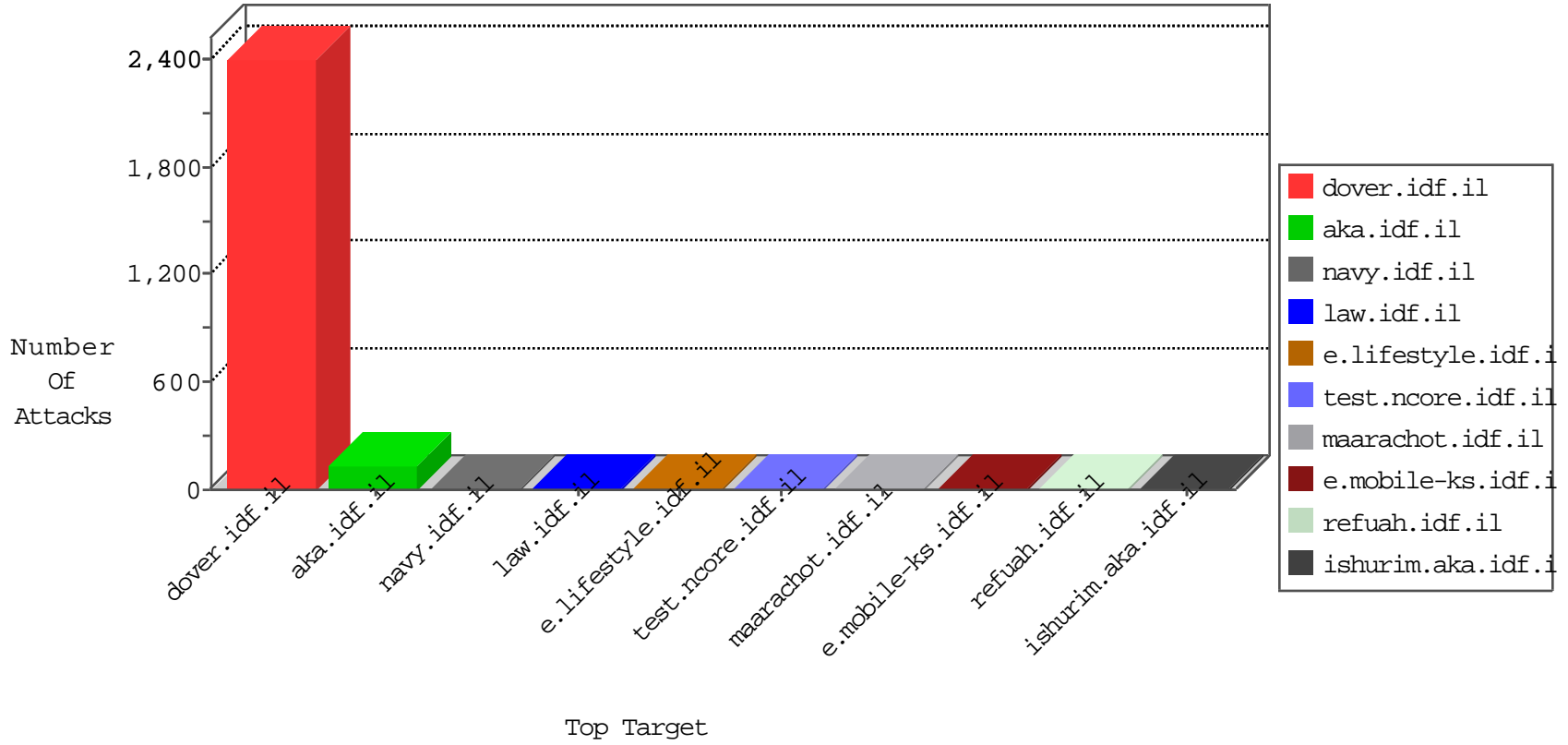
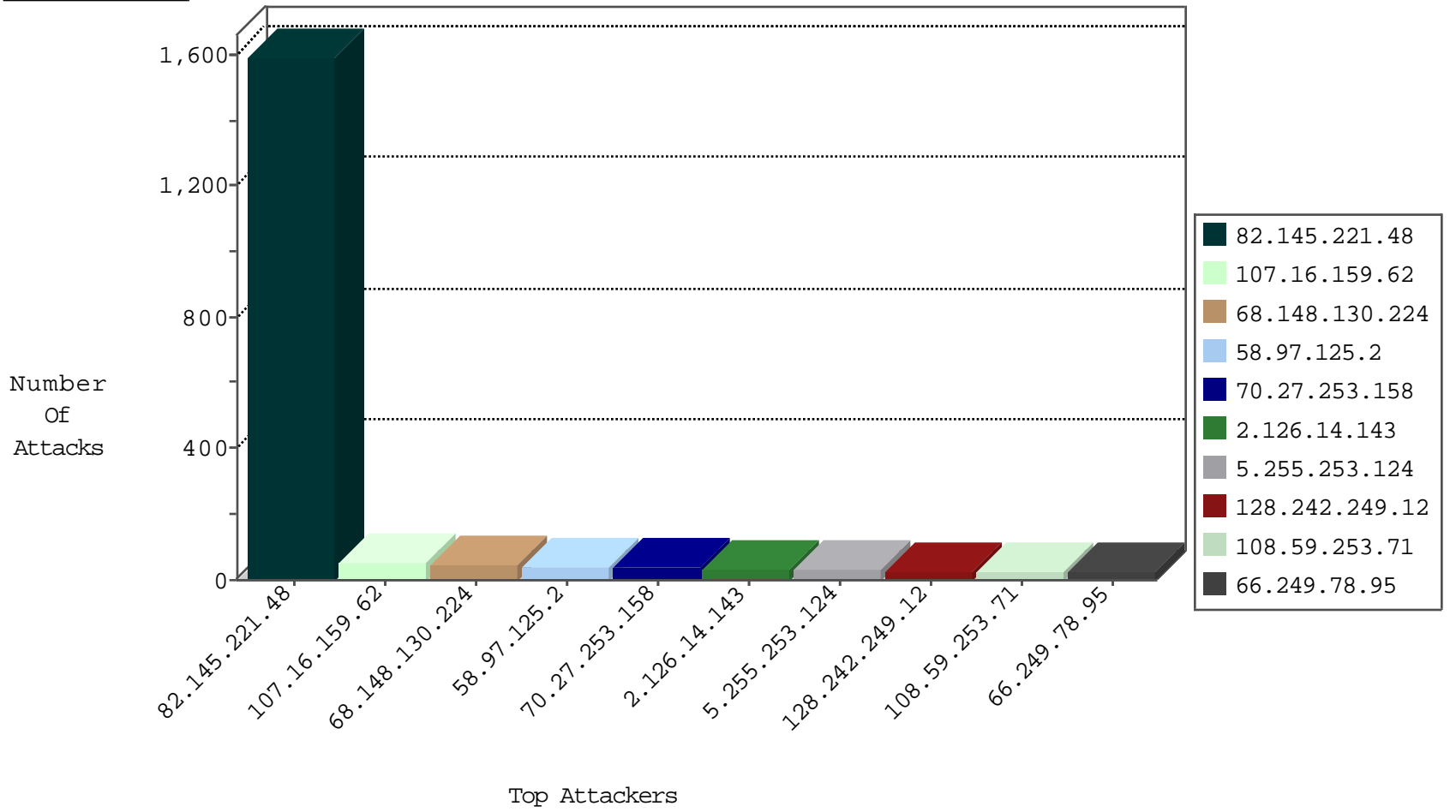


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.111	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	322
219.79.15.197	Hong Kong	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	4
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
83.222.114.116	Russian Federation	147.237.8.28	e.mobile-ks.idf.il	L4 Source or Dest Port Zero	drop	2
204.42.253.130	United States	147.237.76.34	yohanan.idf.il	Block_Udp_All_Nets	drop	2

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	24
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
50.7.159.11	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.177	noore.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.176	test.noore.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.156	aran.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.177	noore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
5.63.150.76	United Kingdom	147.237.77.235	sviva.idf.il	DVRep_P-N_40-59	Permit	1
188.138.9.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.234.122.112	United States	147.237.72.167	ishurim.aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.72.156	aran.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
85.25.103.50	Germany	147.237.76.200	eitan.aka.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
66.249.75.117	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.3	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.30	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.66	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
43.255.191.165	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
155.94.189.2		147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
122.227.249.250	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
111.203.22.57	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
66.249.78.95	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.165	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
178.19.107.114	Poland	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
122.227.249.250	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
122.227.249.250	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
111.203.22.56	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.165	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
82.145.221.48	Europe	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1594
107.16.159.62	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	53
68.148.130.224	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	42
58.97.125.2	Thailand	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	39
70.27.253.158	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	36
2.126.14.143	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
140.139.231.42	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
192.104.181.247	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
77.125.80.248	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
109.176.70.194	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
192.249.64.249	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
188.120.140.35	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	12
41.33.231.86	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
66.249.78.95	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
31.186.228.95	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
24.114.88.90	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
66.249.78.102	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
31.186.228.63	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
31.186.228.66	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
31.186.228.96	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	8
66.249.78.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
216.223.27.60	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	8
68.194.84.107	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
31.186.228.66	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	8
31.186.228.61	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
165.106.126.53	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
31.186.228.86	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
31.186.228.31	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
107.77.97.58	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
31.186.228.65	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.186.228.95	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
176.12.136.108	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.186.228.170	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
207.241.237.106	United States	147.237.77.216	dover.idf.i	Web Servers Slow HTTP Denial of Service	Web Server Enforcement Violation	reject	6
31.186.228.64	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
207.46.13.52	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
31.186.228.67	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
85.65.153.129	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
31.186.228.91	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
31.186.228.25	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
66.249.78.109	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	alert	4
31.186.228.86	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.60	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.64.68	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1
180.76.5.73	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0211-3.stm	Block	1
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	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16472-he/dover.aspx	Block	1
66.249.69.20	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/gyius/gyius/general.aspx	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.52	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluum/templates/www.behazdaa.org.il	Block	1
66.249.64.4	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
66.249.93.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
217.12.202.39	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.78.28	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/m/	Block	1
66.249.64.98	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
180.76.6.213	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/	Block	1
92.53.125.208	Russian Federation	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-admin/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/nakhal/index.stm	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
66.249.69.36	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/gyius/gyius/general.aspx	Block	1
179.34.40.236		147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
66.249.64.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1362-he/dover.aspx	Block	1
68.142.232.17	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/test/wp-admin/	Block	1
66.249.78.88	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1014-ar/dover.aspx	Block	1
66.249.67.58	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8294-he/navy.aspx	Block	1
188.138.17.205	France	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
157.55.39.4	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/chamatz/home/d...sp	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/april/fatah_activists/index	Block	1
207.46.13.95	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.95	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/gyius/forum/asp/showforum.asp	Block	1
179.34.40.236		147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
66.249.64.46	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/m/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.95	Block	1
66.249.67.74	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/1134-he/navy.aspx	Block	1
188.165.15.13	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/announcements/2004/february/08z.stm	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.asp	Block	1
54.209.60.63	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/announcements/2002/march/12.stm	Block	1
207.46.13.131	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
180.76.4.245	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.64.64	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/mobile/	Block	1
68.180.228.251	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-13633-he/dover.aspx	Block	1
66.249.67.155	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
188.165.15.108	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/8/4148.pdf>	Block	1
157.55.39.115	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
61.135.190.70	China	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1312-he/refuah.aspx	Block	1
207.46.13.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62312	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluum/common/includes/bignewsrnd.asp	Block	1