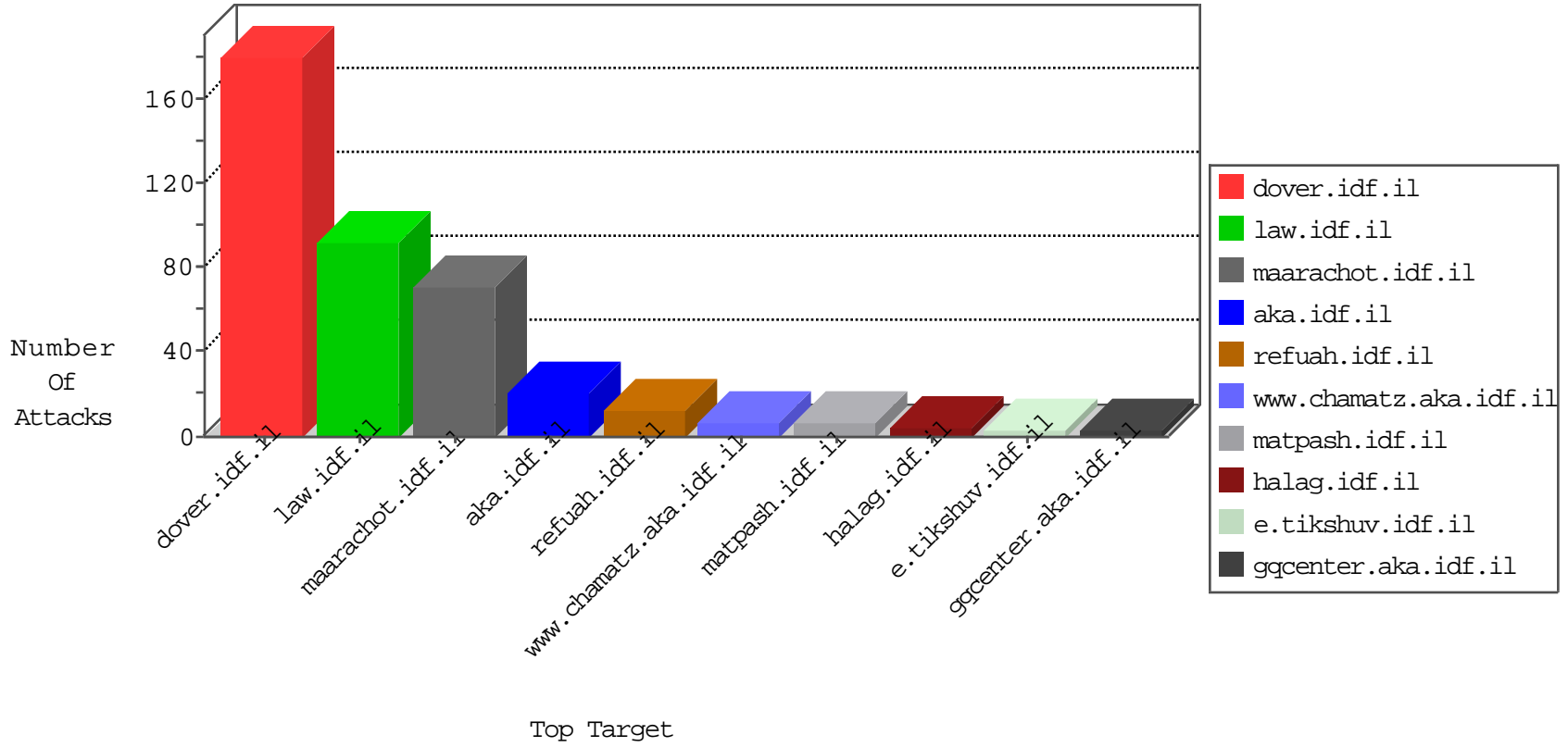
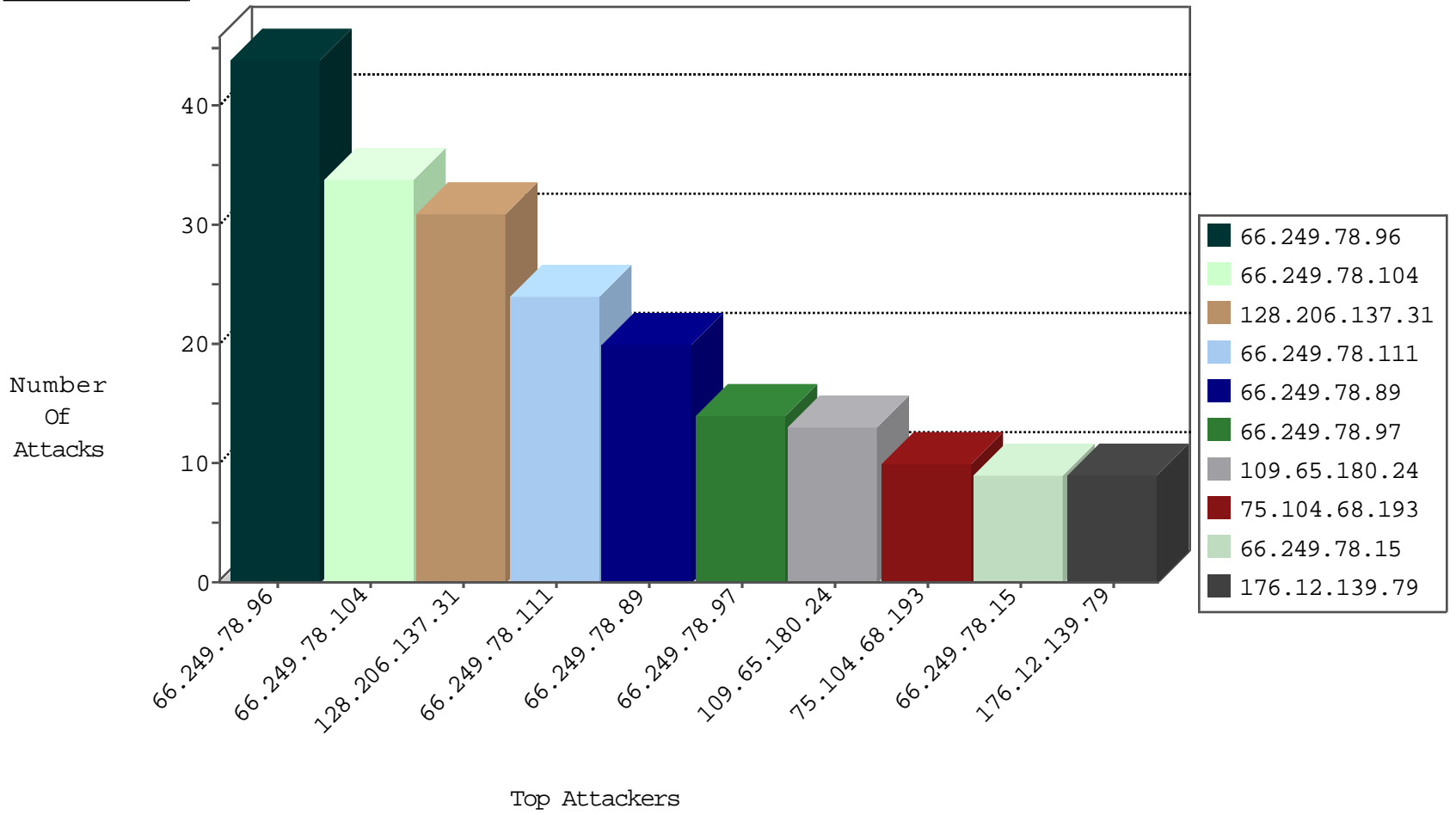




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	8224
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6882
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3211
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2793
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1326
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	432
66.249.78.31	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	368
207.161.151.177	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	255
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	253
220.181.108.141	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	244
66.249.78.2	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	88
66.249.78.38	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	23
24.55.8.171	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
5.29.244.164	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	15
62.210.244.54	France	147.237.77.226	www.chamatz.aka.idf.il	JLM_Purple_Con_Limit_Tcp	drop	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3
66.249.78.29	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2
132.147.93.23	Singapore	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
62.210.244.54	France	147.237.0.34	tikshuv.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
195.37.190.86	Germany	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
62.210.244.54	France	147.237.0.35	akaws.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
181.167.146.47	Argentina	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
66.240.192.138	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
107.183.220.254	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
198.20.70.114	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
119.188.71.175	China	147.237.77.234	halag.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
107.183.220.254	United States	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
188.138.9.50	Germany	147.237.76.148	ggcenter.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	6
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
125.7.102.241	Australia	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
91.224.132.118	Russian Federation	147.237.76.148	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
50.252.197.194	United States	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
199.255.137.52	United States	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -f -sS	1
125.7.102.241	Australia	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
125.7.102.241	Australia	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
91.224.132.118	Russian Federation	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.76.148	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
50.252.197.194	United States	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 4096	1
199.255.137.52	United States	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 2048	1
5.196.147.122	Germany	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
128.206.137.31	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
109.65.180.24	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
75.104.68.193	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
176.12.139.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.69.32	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
172.10.98.174	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
2.28.192.87	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
84.109.200.185	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
80.246.133.87	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
64.236.82.2	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
185.13.193.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.47.246	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.246.133.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.93.164	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.186.120.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
74.90.244.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
113.159.159.59	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
176.12.146.26	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.65.160.147	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
149.78.245.101	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
92.64.90.134	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unexpected post SYN packet - RST or SYN expected	drop	drop	1
41.34.137.144	Egypt	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
37.140.141.38	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
154.5.108.251	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
107.170.144.19	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
207.46.13.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
5.153.43.35	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
84.109.31.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
107.183.220.254	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
41.34.137.144	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
63.249.66.212	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
212.235.68.141	Israel	147.237.77.243	mobile.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	1
37.26.148.202	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
85.65.17.145	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
41.34.137.144	Egypt	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
178.137.85.64	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	4
207.46.13.131	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
107.183.220.254	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
37.142.131.93	Israel	147.237.72.166	aka.idf.il	Distributed 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
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.58.74.139	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
85.65.17.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
5.29.244.164	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.78.89	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchfText in www.law.idf.il/275-he/patzar.aspx	None	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.48	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/giyus.asp	Block	1
54.161.135.168	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/120403-2.stm	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
66.249.75.66	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/may/hamas.stm	Block	1
66.249.64.93	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1072-he/nakhal.aspx	Block	1
178.137.85.64	Ukraine	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.69.85	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/23012011yezu.aspx	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 54.245.64.111	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/requestsinfo.asp	Block	1
69.16.197.134	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
66.249.75.74	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/2004/january/0127-1.stm	Block	1
66.249.69.24	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/929-he/refuah.aspx	Block	1
107.183.220.254	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 107.183.220.254	Block	1
37.231.251.192	Kuwait	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/163-6941-en/patzar.aspx	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp?moduleid=2&catid=22703&docid=22716	Block	1
66.249.75.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.58	Block	1
54.245.64.111	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
157.55.39.45	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/940-he/patzar.aspx	Block	1
66.249.75.104	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/m/	Block	1
207.46.13.14	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/994-he/patzar.aspx	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
107.183.220.254	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ckeditor/ckfinder/core/connector/asp/connector.asp	Block	1
46.105.218.1	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/sep	Block	1
65.75.160.133	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
157.55.39.64	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/602-2267-he/patzar.aspx	Block	1
72.29.127.15	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
66.249.78.9	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.40	Block	1
54.161.135.168	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
66.249.75.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.66	Block	1
66.249.64.71	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1