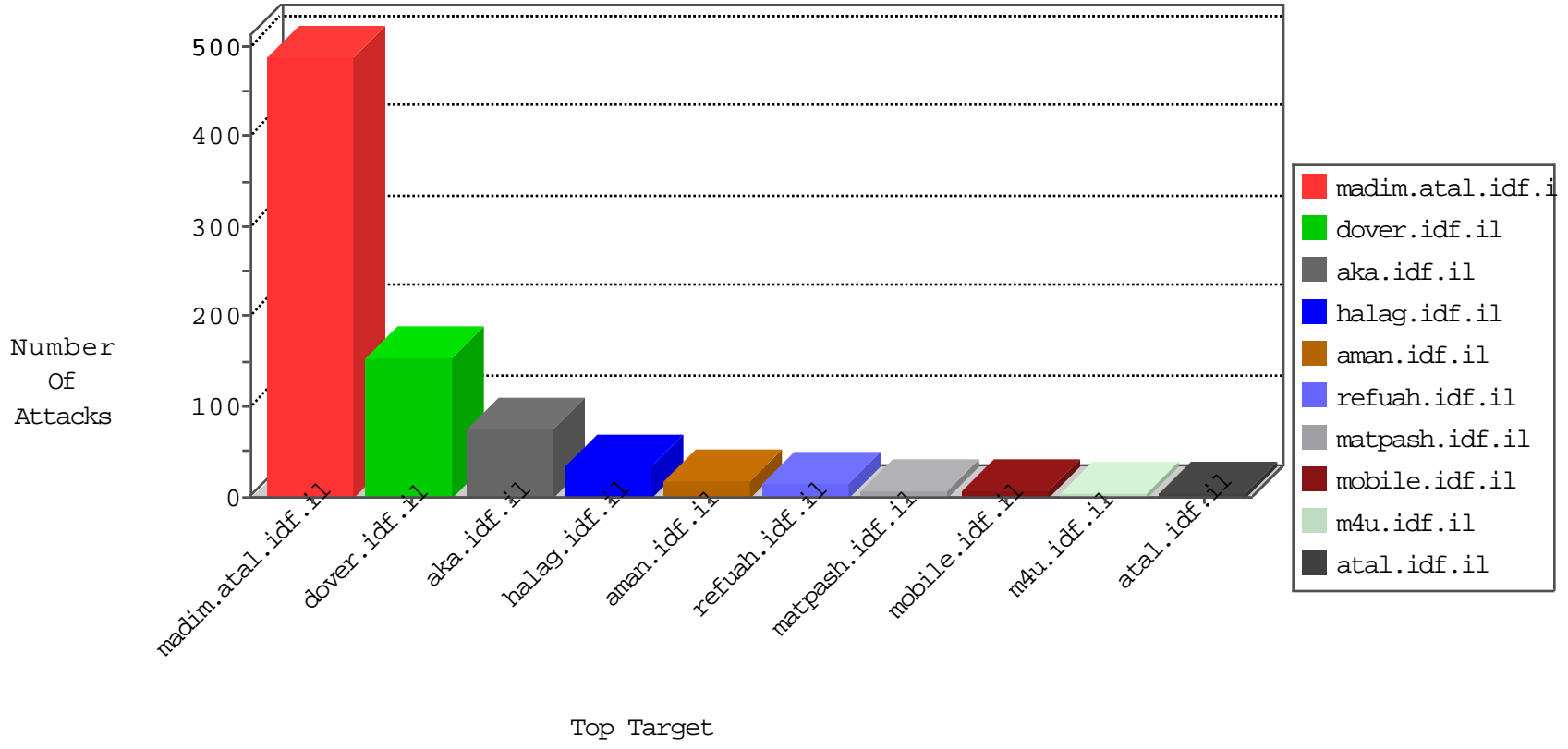
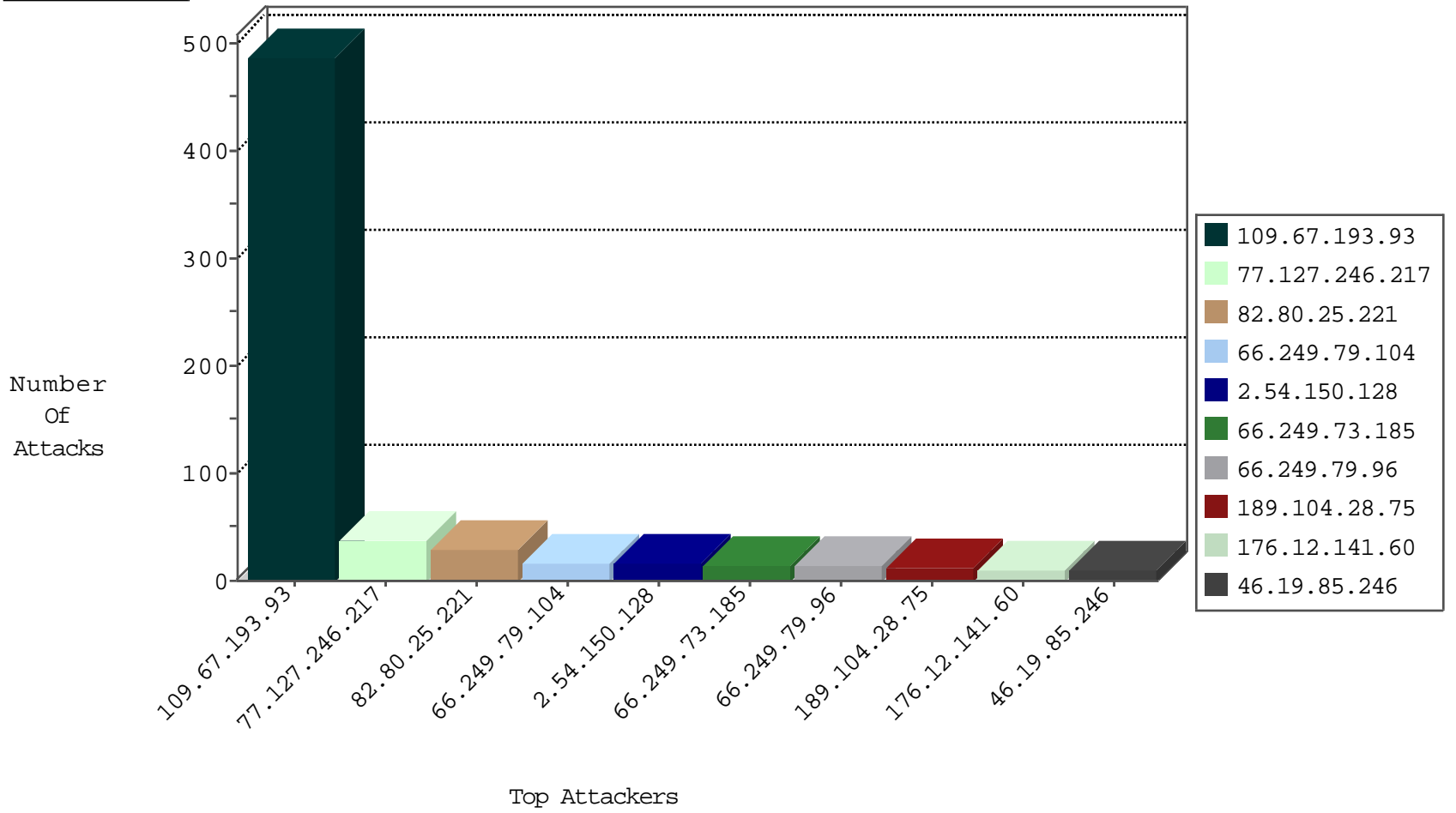




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
------------------	------------------	----------------	----------	-----------	---------------	-------

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.65.195.136	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.187.129.166	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
176.67.123.227	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.150	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
77.127.246.217	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

## 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	29
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
89.138.11.240	Israel	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	4
217.132.123.238	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.73.220	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.7	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
162.244.24.233		147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
115.238.55.163	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
5.196.248.85	Germany	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.44	e.refuah.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
61.240.144.64	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
183.136.216.7	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
162.244.24.233		147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
162.244.24.233		147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
115.238.55.163	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
41.200.39.102	Algeria	147.237.77.216	dover.idf.il	SERVER-WEBAPP Mambo upload.php access	1
82.117.208.243		147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
221.226.106.188	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
77.127.246.217	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	35
66.249.79.104	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
66.249.79.96	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
66.249.73.185	United States	147.237.77.216	doover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
176.12.141.60	Israel	147.237.77.216	doover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
46.19.85.246	Israel	147.237.77.216	doover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
176.12.151.209	Israel	147.237.77.216	doover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
66.249.73.193	United States	147.237.77.216	doover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.73.201	United States	147.237.77.216	doover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.135.14	Israel	147.237.77.216	doover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.140.78	Israel	147.237.77.216	doover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
2.54.150.128	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	alert	5
46.19.85.191	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
2.54.150.128	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
2.54.150.128	Israel	147.237.72.156	aman.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
5.102.254.246	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
37.247.36.84	Netherlands	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
189.104.28.75	Brazil	147.237.77.216	doover.idf.il	First packet isn't SYN	drop	drop	4
66.249.79.112	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
5.22.129.254	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
189.104.28.75	Brazil	147.237.77.216	doover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.173	Israel	147.237.77.216	doover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
189.104.28.75	Brazil	147.237.77.216	doover.idf.il	Unexpected post SYN packet - RST or SYN expected	drop	drop	2
46.19.85.173	Israel	147.237.77.216	doover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.121.121.227	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
5.102.254.246	Israel	147.237.77.226	www.chamatz.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
41.200.39.102	Algeria	147.237.77.216	doover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.156	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
207.241.237.223	United States	147.237.77.216	doover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
157.55.39.42	United States	147.237.77.216	doover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
8.37.227.68	Anonymous Proxy	147.237.77.216	doover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	2
46.19.85.246	Israel	147.237.77.216	doover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
141.212.122.200	United States	147.237.76.148	ggcenter.aka.idf.il		drop	drop	1
37.247.36.67	Netherlands	147.237.76.200	eitan.aka.idf.il		drop	drop	1
94.159.141.180	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
77.127.106.95	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
176.12.136.110	Israel	147.237.77.216	doover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.141	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
122.224.121.147	China	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
85.64.247.169	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.201	United States	147.237.76.197	e.himush.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
109.64.188.163	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.150	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.44	United States	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
85.65.79.79	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
193.37.152.241	Germany	147.237.77.216	doover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
141.212.122.209	United States	147.237.76.200	eitan.aka.idf.il		drop	drop	1
109.226.60.101	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
77.237.138.51	Czech Republic	147.237.77.19	law-forum.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
62.90.122.230	Israel	147.237.72.167	ishurim.aka.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
109.67.193.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	487
89.138.224.74	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 89.138.224.74	Block	3
84.228.58.78	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
157.55.39.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.42	Block	3
176.12.138.58	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.181.131.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.16	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.16	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
85.64.70.49	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
93.173.233.161	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
204.28.105.82		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.stm	Block	2
41.200.39.102	Algeria	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
125.209.235.184	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
85.65.26.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authentication-service.asmx/getuserdetails	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	Double URL Encoding - parameter: in www.idf.il/hebrew/organization/patzar/atar1/mlsl/pirsumim/journal/15%5caviram15.doc	Block	1
46.19.85.224	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
109.65.99.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
66.249.75.7	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/modiin/default.aspx	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	1
142.54.183.130	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18092-en/dover.aspx/trackback/	Block	1
176.12.144.155	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.225	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.75.15	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/pazan/iftah.stm	Block	1
157.55.39.6	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	1
5.29.149.123	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authentication-service.asmx/getuserdetails	Block	1
89.138.224.74	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
207.46.13.30	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/captcha.ashx	Block	1
77.127.106.95	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
176.67.123.227	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//894-ar	Block	1
66.249.69.36	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
109.253.159.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
66.249.75.34	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
193.37.152.241	Germany	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	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/june/22.stm	Block	1
31.31.26.107	Moldova, Republic of	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/brothers/skira/default.asp	None	1
213.57.133.71	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
77.127.246.217	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 77.127.246.217	Block	1
180.76.4.180	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.69.50	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
115.25.81.70	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
85.64.119.110	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0501-1.stm	Block	1
95.153.184.235	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter in www.aka.idf.il/brothers/skira/default.asp	None	1
77.237.138.51	Czech Republic	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /	Block	1
66.249.69.127	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/modiin/default.aspx	Block	1
188.165.15.176	France	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 188.165.15.176	Block	1