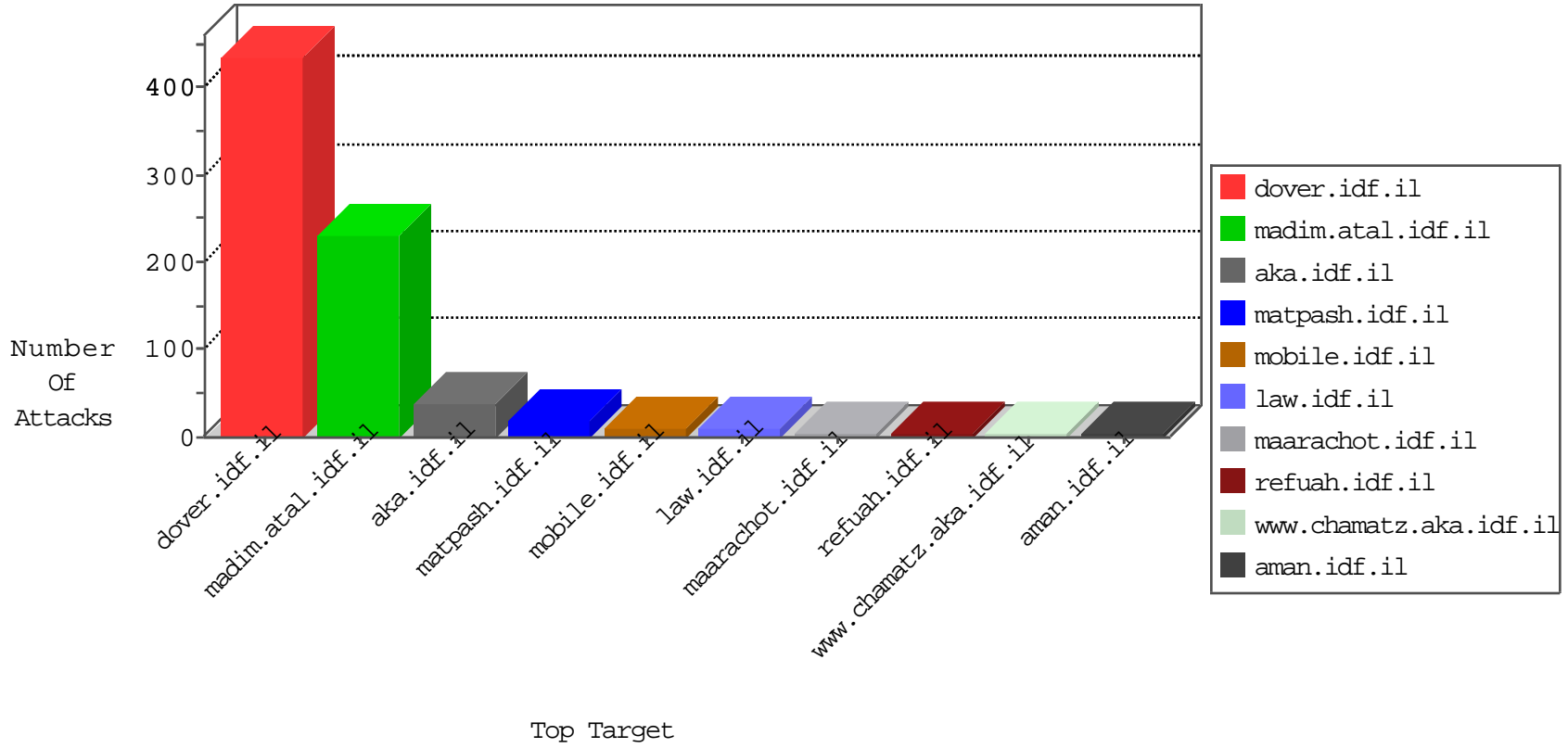
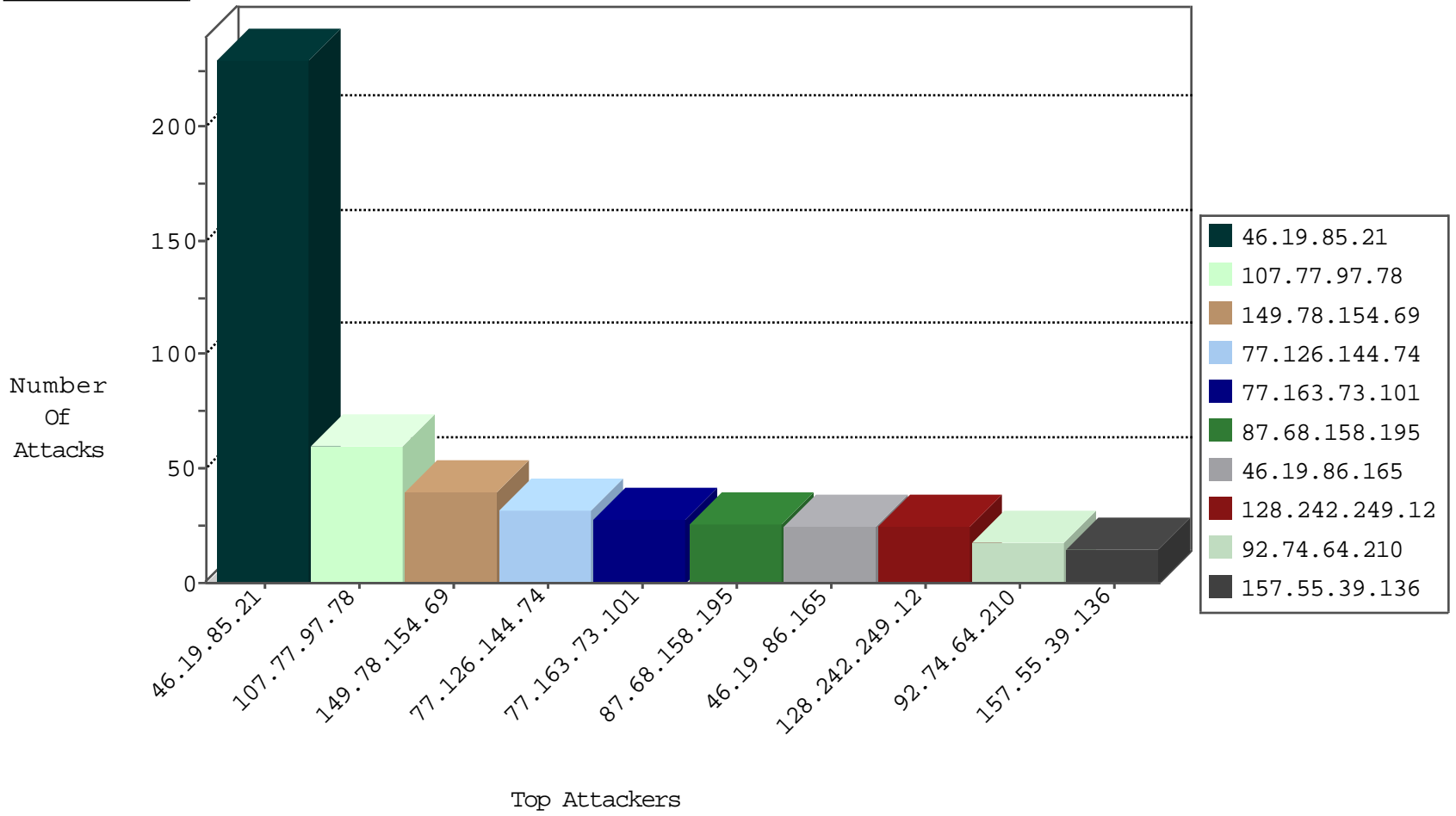


Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.22	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	645
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	496
46.19.86.165	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	19
46.19.86.165	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	19
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
109.64.10.34	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
66.240.192.138	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
195.37.190.86	Germany	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1

## 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	25
85.25.103.50	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	2
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
79.177.109.165	Israel	147.237.77.170	maarachot.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
2.54.152.36	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
200.37.4.201	Peru	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.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
93.114.44.187	Anonymous Proxy	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
220.181.125.15	China	147.237.77.170	maarachot.idf.il	C103: HTTP: User Agent Sogou+web+spider	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	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1

## Top Attackers In IDF

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
66.249.78.22	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	4
218.89.137.3	China	147.237.72.217	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.67	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
221.235.189.245	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.53	Moldova, Republic of	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.130		147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 4096	1
221.235.189.245	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
82.117.208.243		147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
201.239.118.143	Chile	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
194.63.141.166	Russian Federation	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.76.148	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
128.199.238.136	Singapore	147.237.72.166	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
221.235.189.245	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
107.77.97.78	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	60
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	34
77.126.144.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	32
77.163.73.101	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
87.68.158.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
92.74.64.210	Germany	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	18
85.114.119.251	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.19.85.21	Israel	147.237.0.19	madim.atal.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
157.55.39.136	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
200.37.4.201	Peru	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
190.229.126.218	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
37.26.146.209	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
73.185.35.138	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.253.149.81	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
24.203.59.13	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
84.228.165.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.65.97.23	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
85.130.222.38	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	3
84.111.15.51	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
109.64.10.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
82.132.219.207	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.192	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
77.127.243.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.109.110.224	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
193.189.143.162	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
99.238.32.134	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.109.204.35	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.250.102.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
78.128.78.164	Bulgaria	147.237.72.166	aka.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
188.165.15.99	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
149.78.101.88	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
79.177.109.147	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
5.29.164.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
213.8.129.141	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.89.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	218
2.52.28.147	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	10
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	8
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	7
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	6
93.172.3.151	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	4
46.253.81.140	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	3
66.249.78.82	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	2
66.249.64.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.238	Block	2
212.179.42.241	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	2
46.116.243.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	2
93.172.3.151	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 93.172.3.151	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.224	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
188.165.15.230	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8766-he/refuah.aspx	Block	1
66.249.75.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
195.154.211.220	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/default.aspx	Block	1
67.84.76.182	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/pazan/pazan.stm	Block	1
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
54.163.100.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/iaf/present4.stm	Block	1
94.153.9.66	Ukraine	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
66.249.78.89	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
2.52.28.147	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
79.177.18.77	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteyerua/	Block	1
54.167.183.116	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
142.54.161.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17055-en/dover.aspx/trackback/	Block	1
66.249.67.206	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1356-he/refuah.aspx	Block	1
207.46.13.26	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
79.177.109.165	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.75.109	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/reserve/	Block	1
66.249.64.219	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.36	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1