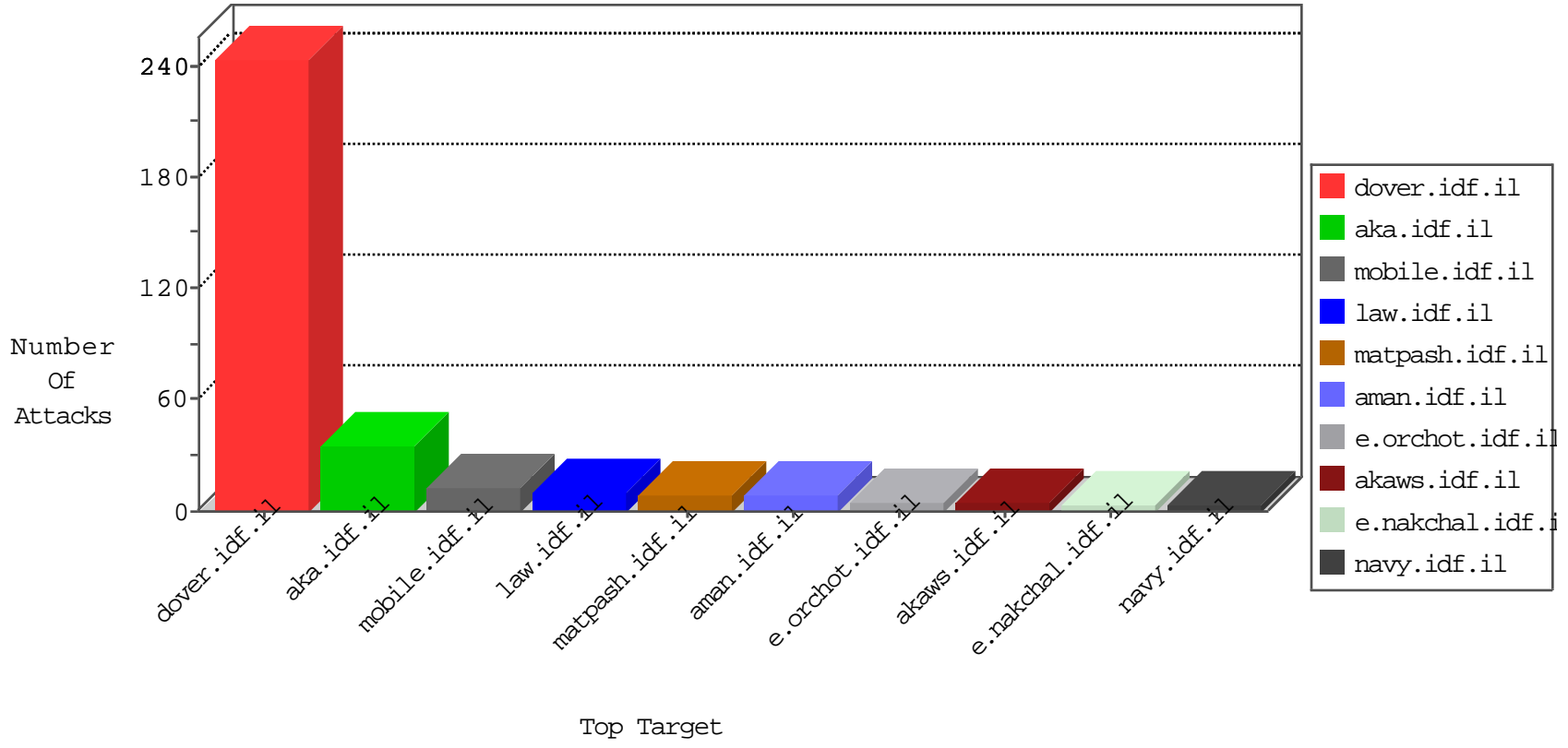
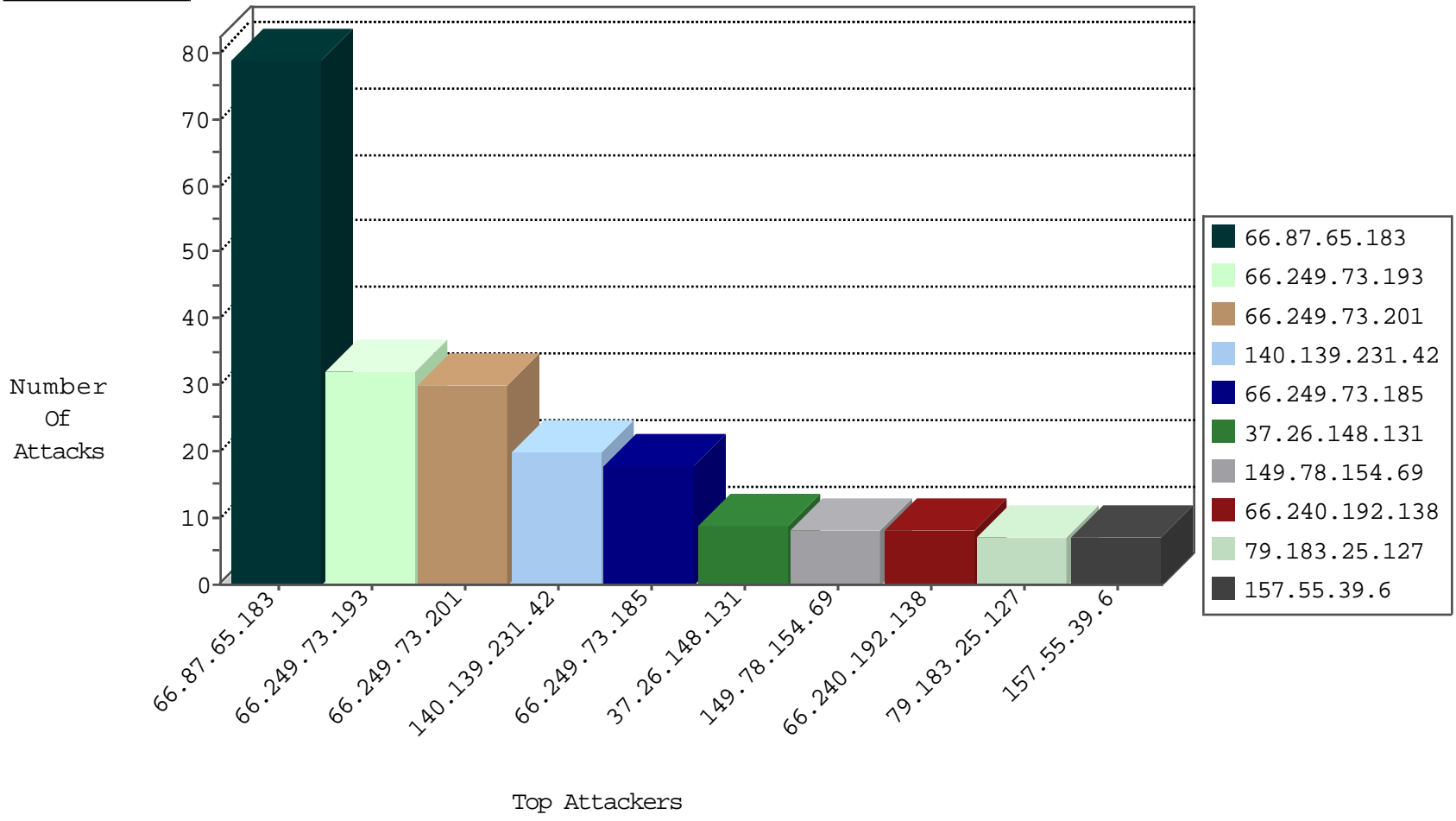




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
198.20.69.98	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	2
198.20.69.98	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.34	tikshuv.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
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.46	e.chimuch.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
198.20.69.98	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.198	e.yohalan.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
198.20.70.114	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
104.204.204.227		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.19	madim.atal.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	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
220.181.125.15	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	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
61.240.144.67	China	147.237.76.44	e.refuah.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
208.88.126.186	United States	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
52.7.7.145	United States	147.237.0.16	ny-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
178.19.107.114	Poland	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
50.252.197.194	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
167.88.43.110		147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
167.88.43.110		147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
162.248.10.134	Canada	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
144.0.0.60	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
50.252.197.194	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
168.187.246.41	Kuwait	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
167.88.43.110		147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
167.88.43.110		147.237.0.35	akaws.idf.il	ET SCAN NMAP -f -sS	1
162.248.10.134	Canada	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 3072	1
144.0.0.60	China	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.87.65.183	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	79
66.249.73.201	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
140.139.231.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
37.26.148.131	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
157.55.39.6	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
77.127.158.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
62.210.162.148	France	147.237.77.74	law.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	3
128.242.249.11	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.65.45.127	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
5.28.186.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.16	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.162	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
89.139.164.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
173.252.110.113	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
95.211.168.135	Netherlands	147.237.8.27	e.madim.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
37.140.141.37	Russian Federation	147.237.77.74	law.idf.il	SAM rule	drop	drop	1
146.185.239.104	Russian Federation	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.86.16	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
176.12.140.158	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
98.210.231.138	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
79.177.15.63	Israel	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
31.210.186.235	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
209.85.238.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
107.170.181.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
41.37.107.67	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
80.82.78.186	Netherlands	147.237.0.33	idf.il		drop	drop	1
32.212.249.5	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
212.98.152.56	Lebanon	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
218.22.211.69	China	147.237.77.61	e.cogat.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
73.47.154.189	United States	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
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	7
79.183.25.127	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	7
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	5
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
46.117.94.164	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	4
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	4
85.186.88.38	Romania	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
178.137.19.143	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	2
85.214.94.252	Germany	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
41.44.174.255	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/894-ar	Block	2
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.186.88.38	Romania	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	1
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
109.186.59.56	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	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
176.12.141.86	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.67.91	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71926-he/maarachot.aspx	Block	1
27.34.91.174	Nepal	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/earthquakes.stm	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/faq.aspx	None	1
207.241.229.213	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/62532.pdf?g2=whvq9jgvov3igm-oflegda	Block	1
62.210.162.148	France	147.237.77.74	law.idf.il	Admin Blocking	Block	1
109.186.59.56	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	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
66.249.67.92	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/320-6455-he/patzar.aspx	Block	1
37.19.118.24	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.214.94.252	Germany	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
220.181.108.76	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.219	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
136.243.36.97	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 136.243.36.97	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
180.76.6.134	China	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/shared/clientscripts/submodal/'+ gdefaultpage +'	Block	1
37.57.231.112	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/656-en/	Block	1
157.55.39.117	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
66.249.78.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/62281	Block	1
66.249.65.97	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	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
85.64.67.84	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/terms.aspx	None	1
199.30.24.168	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.64.135.166	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/speakerofmatpash/pages/summaryofgazainternationalorganizations.aspx	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/1124-4.stm	Block	1
66.249.67.79	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-4883-he/patzar.aspx	Block	1