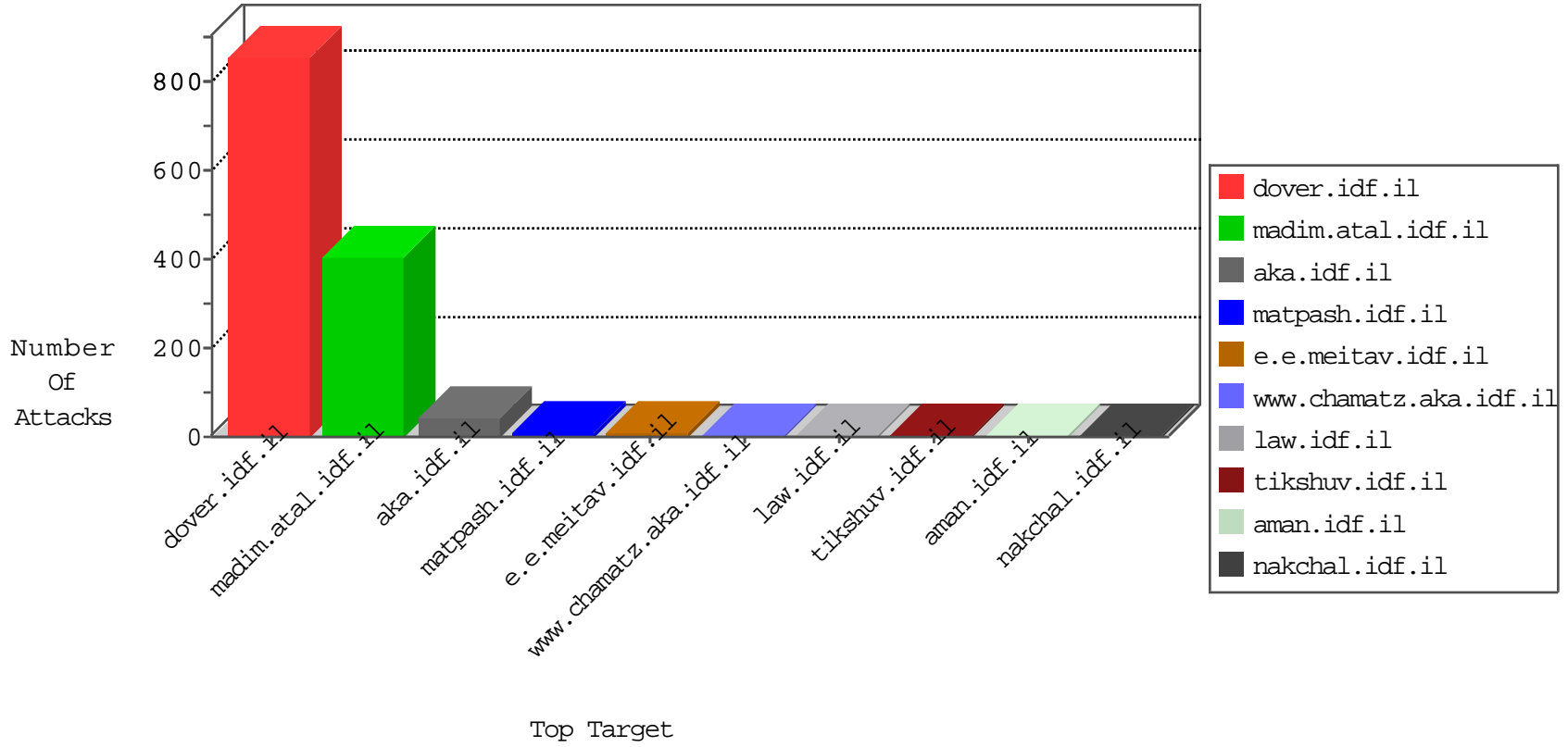
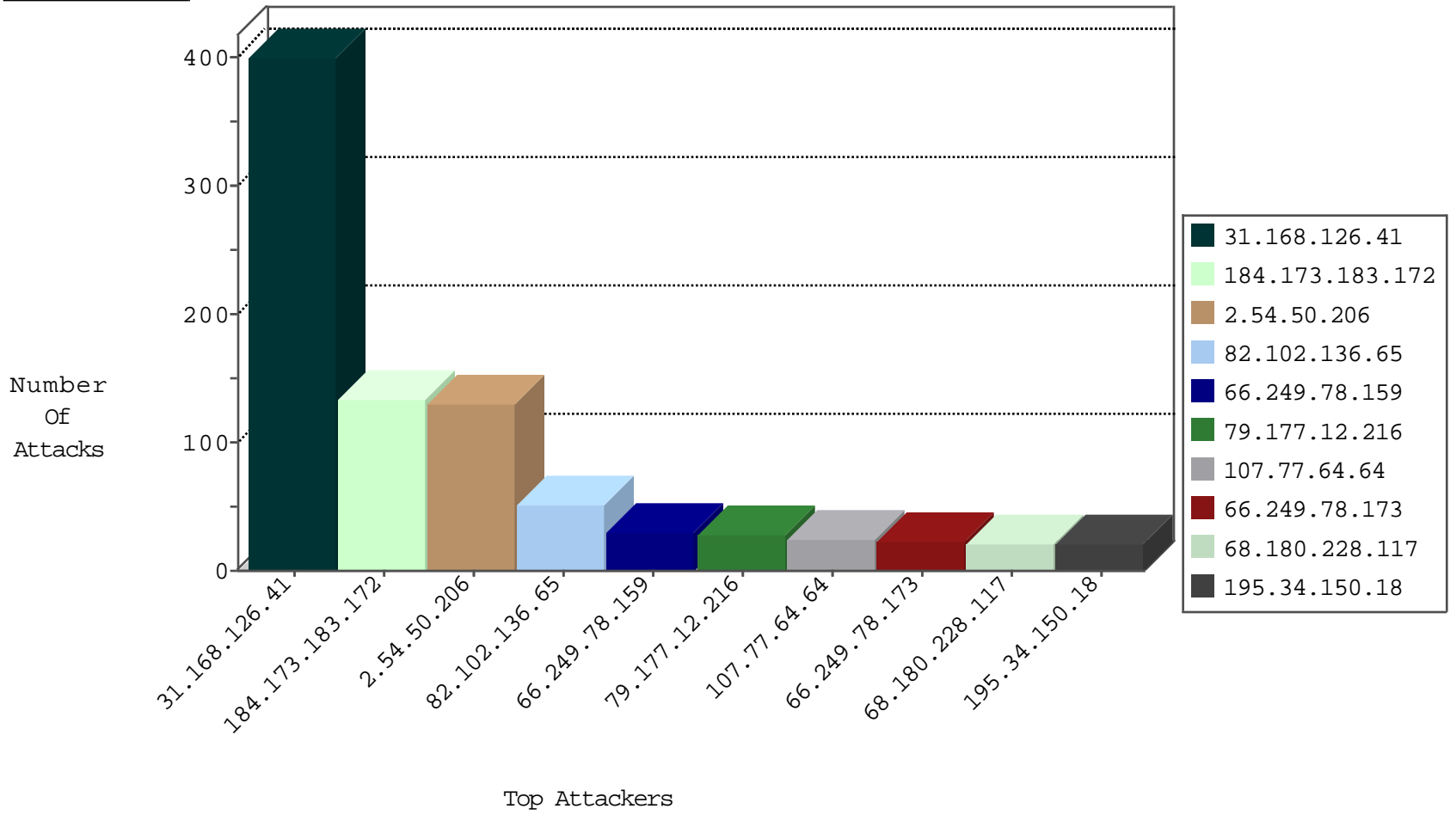


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
188.0.16.174	Russian Federation	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	6
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
85.64.63.37	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
66.240.236.119	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	133
122.2.21.141	Philippines	147.237.77.176	matpash.idf.il	Cl000108: HTTP: Trying to locate existing FCKeditor	Block	4
46.117.221.59	Israel	147.237.0.34	tikshuv.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
197.33.124.239	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
198.20.69.98	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
24.90.111.185	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
74.5.137.100	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
50.7.159.11	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.196	e.sviva.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

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
79.138.70.153	Sweden	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.68	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.138.70.153	Sweden	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.68	China	147.237.76.30	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.67	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
199.231.185.135	United States	147.237.77.227	e.haraz.idf.il	ET SCAN NMAP -sS window 2048	1
58.20.54.249	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.16.206	Russian Federation	147.237.72.14	dover.idf.il(old)	ET DROP Spamhaus DROP Listed Traffic Inbound	1
167.114.40.66	United States	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
167.114.40.66	United States	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
79.138.70.153	Sweden	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.68	China	147.237.76.86	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.138.70.153	Sweden	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.68	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.138.70.153	Sweden	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.68	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	China	147.237.77.227	e.haraz.idf.il	ET SCAN NMAP -sS window 1024	1
199.231.185.135	United States	147.237.77.227	e.haraz.idf.il	ET SCAN NMAP -f -sS	1
193.107.16.206	Russian Federation	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
167.114.40.66	United States	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
167.114.40.66	United States	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
82.214.114.5	Macedonia, the Former Yugoslav Republic of	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.54.50.206	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	130
82.102.136.65	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	51
79.177.12.216	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	27
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
107.77.64.64	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
68.180.228.117	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
79.180.227.159	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
216.189.31.119	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
50.200.254.195	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
66.249.64.76	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.78.166	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
212.76.127.111	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
31.44.143.197	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
208.54.36.191	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
87.68.39.165	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	9
79.178.14.59	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
209.6.236.151	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
84.228.192.24	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
212.76.127.212	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
89.138.240.218	Israel	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	6
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
186.158.218.156	Argentina	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
91.64.66.147	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
89.138.240.218	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	6
176.12.147.59	Israel	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	5
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
208.69.40.107	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
213.205.239.97	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
176.12.147.59	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	5
82.102.136.70	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
217.230.34.136	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
109.65.37.38	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
65.19.138.34	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
79.182.49.92	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
69.120.132.123	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
71.192.122.47	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
72.89.80.31	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
87.68.231.0	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
66.249.78.95	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	3
74.162.132.234	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
66.249.78.102	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	3
46.117.221.59	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
89.139.51.131	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
77.125.119.104	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
31.168.126.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	401
46.117.40.91	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	7
46.117.40.91	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/updateuserdetails.aspx	Block	4
79.180.2.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	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	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
178.137.166.68	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	2
66.249.64.73	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/console/core/doc_mgr/undefined	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
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
162.248.244.253	United States	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
66.249.64.66	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
77.66.121.237	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/048.stm	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216//templates/sendtofriend/sendtofriend.aspx	Block	1
66.249.67.84	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/1/1381.pdf	Block	1
141.212.122.26	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fr.hamaz	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.68	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
5.102.254.96	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
77.126.0.46	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19657-he/dover.aspx	Block	1
66.249.67.92	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	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
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/default.aspx 	Block	1
207.46.13.7	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/994-7806-he/nakhal.aspx	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/himuch	Block	1
157.55.39.183	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1111-7808-he/nakhal.aspx	Block	1
61.135.190.201	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	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
207.46.13.43	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1117-7807-he/nakhal.aspx	Block	1
66.249.64.73	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1133-he/atal.aspx	Block	1
37.26.148.136	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//894-ar	Block	1
85.250.125.191	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/soldiercontact.aspx	None	1
66.249.75.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
162.248.244.253	United States	147.237.77.74	law.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 147.237.77.216/1613-15488-he/dover.aspx	Block	1
77.66.121.237	Denmark	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18340-he/dover.aspx	Block	1
66.249.64.77	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
89.107.186.233	Germany	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1