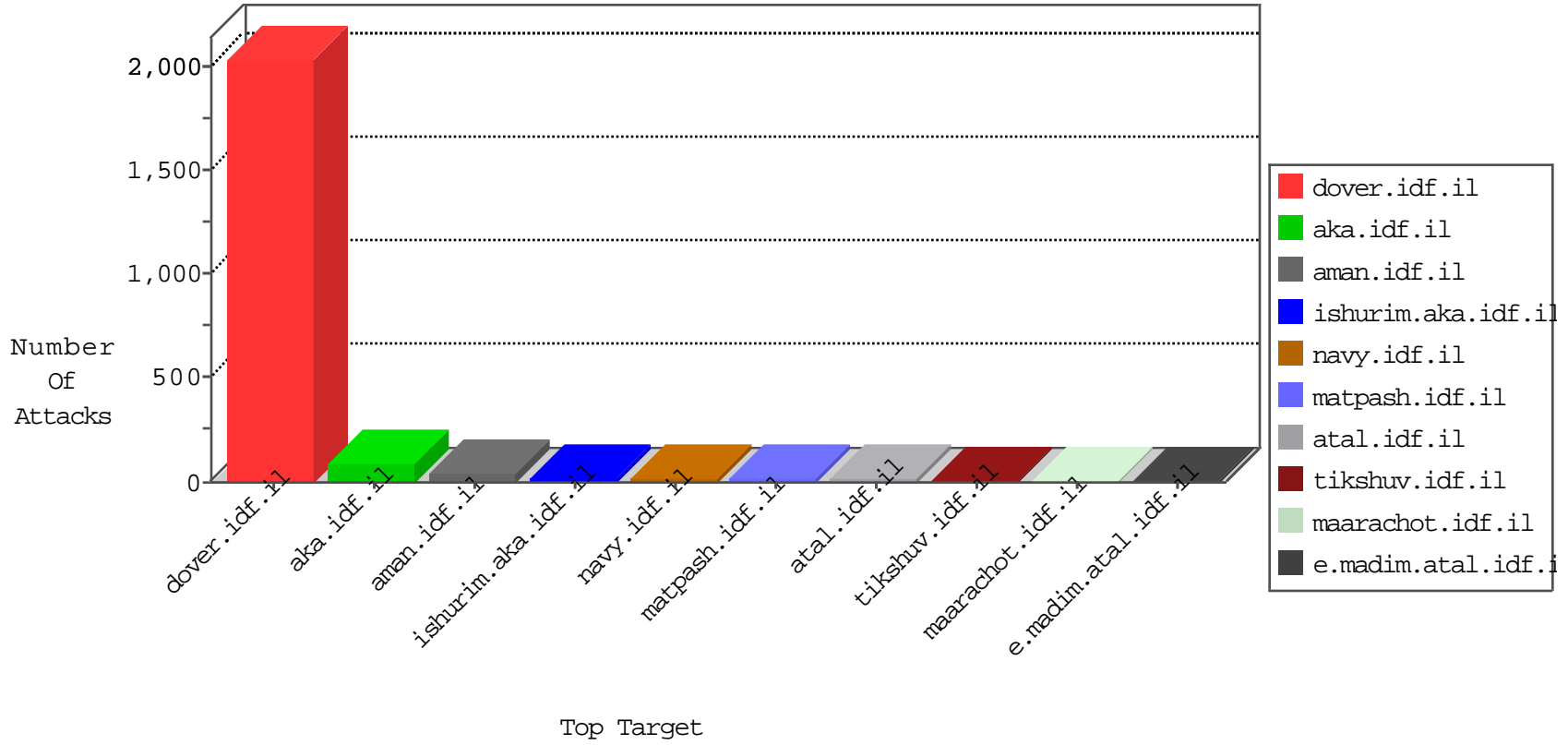
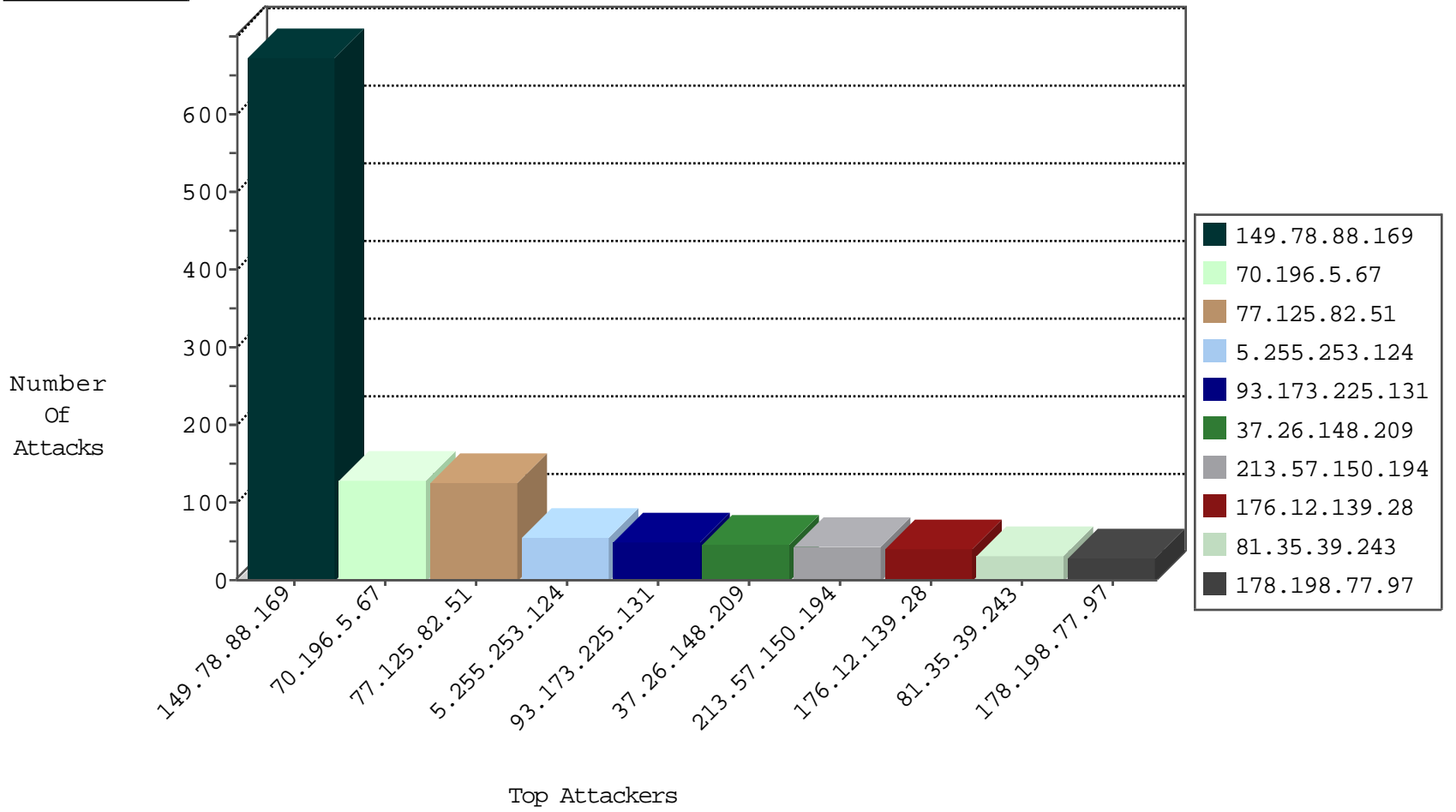


Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
93.172.101.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	183
213.57.150.194	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	142
213.57.150.194	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	123
46.117.20.86	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
37.142.128.154	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	89
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
123.202.81.159	Hong Kong	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
111.202.66.66	China	147.237.8.27	e.madim.atal.idf.il	L4 Source or Dest Port Zero	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	9
71.6.165.200	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.156	aman.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
93.173.142.227	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
208.180.240.62	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.135.131	United States	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
79.180.251.52	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.16	ny-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
79.182.132.66	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.192.138	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.27	e.madim.atal.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
85.25.103.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.31	nakchal.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
66.249.65.55	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
93.173.181.182	Israel	147.237.0.34	tikshuv.idf.il	LOCAL RULES DOS attack 01/2012	2
176.12.150.133	Israel	147.237.0.34	tikshuv.idf.il	LOCAL RULES DOS attack 01/2012	2
66.249.67.139	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
84.94.60.40	Israel	147.237.0.34	tikshuv.idf.il	LOCAL RULES DOS attack 01/2012	2
66.249.78.93	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
123.136.24.60	Bangladesh	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
123.136.24.60	Bangladesh	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
60.18.162.244	China	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
123.136.24.60	Bangladesh	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
123.136.24.60	Bangladesh	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
210.61.150.154	Taiwan	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 3072	1
121.46.0.125	China	147.237.76.34	yochalan.idf.il	ET SCAN NMAP -sS window 3072	1
178.19.107.114	Poland	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243		147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
78.134.240.185	Croatia	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
123.136.24.60	Bangladesh	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
123.136.24.60	Bangladesh	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
123.136.24.60	Bangladesh	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
60.18.162.244	China	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
123.136.24.60	Bangladesh	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
211.149.240.162	China	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
123.136.24.60	Bangladesh	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	United States	147.237.77.74	law.idf.il	ET DROP Dshield Block Listed Source	1
121.46.0.125	China	147.237.76.34	yochalan.idf.il	ET SCAN NMAP -sS window 1024	1
192.64.83.219	United States	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
178.19.107.114	Poland	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
78.134.240.185	Croatia	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
123.136.24.60	Bangladesh	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
149.78.88.169	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	675
70.196.5.67	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	129
77.125.82.51	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	125
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
93.173.225.131	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	48
37.26.148.209	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	47
176.12.139.28	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	41
178.198.77.97	Switzerland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	29
46.19.85.179	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	28
84.228.148.22	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	26
81.35.39.243	Spain	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
166.216.157.30	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
207.200.211.206	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	21
62.219.154.133	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	20
46.121.214.149	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
208.221.239.4	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
216.113.160.72	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
66.249.78.173	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
79.181.27.135	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	16
62.219.154.129	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
66.249.78.159	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
62.219.154.139	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
27.153.173.169	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
213.57.150.194	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	12
46.116.6.223	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
96.26.132.153	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
109.67.37.138	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
46.19.85.158	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	10
188.120.148.177	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	10
85.65.145.42	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
84.51.154.109	United Kingdom	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
178.252.189.48	Iran, Islamic Republic of	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
185.4.253.18	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
195.34.150.18	Austria	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
128.242.249.10	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
203.127.58.236	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
149.78.174.142	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
84.109.2.148	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
119.73.253.4	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
220.255.1.161	Singapore	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
84.110.2.193	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
84.228.131.240	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
81.35.39.243	Spain	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
220.255.1.142	Singapore	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
79.181.7.88	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
178.252.189.48	Iran, Islamic Republic of	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
84.228.83.136	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.182.22.155	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-18139-en/dover.aspx	Block	1
180.76.6.40	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/born5.stm	Block	1
50.243.68.162	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/gilui/site/english/main_index.stm	Block	1
85.64.66.145	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
66.249.67.91	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
213.57.143.158	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
79.182.132.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter pop in www.aka.idf.il/main/home/	None	1
185.32.177.126	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/tems.aspx	None	1
66.249.64.145	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/general.aspx	Block	1
85.65.170.17	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.253	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1086-he/atal.aspx	Block	1
157.55.39.227	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-	Block	1
79.182.132.66	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
188.138.17.205	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
66.249.64.150	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
109.65.74.196	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/938-he/cogat.aspx	Block	1
66.249.81.227	Israel	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/./favicon.ico	Block	1
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/modules/forums/forum.aspx	Block	1
157.82.156.135	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
2.54.35.38	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
84.110.8.37	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https://www.aka.idf.il/	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	1
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal/natziv4.stm	Block	1
188.165.15.85	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
149.78.149.184	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/humanitarianarchive.stm	Block	1
66.249.78.73	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
180.76.5.187	China	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.120.98.76	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
66.249.65.1	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/speakerofmatpash/pages/summaryofga zainternationalorganizations.aspx	Block	1
198.20.69.74	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1