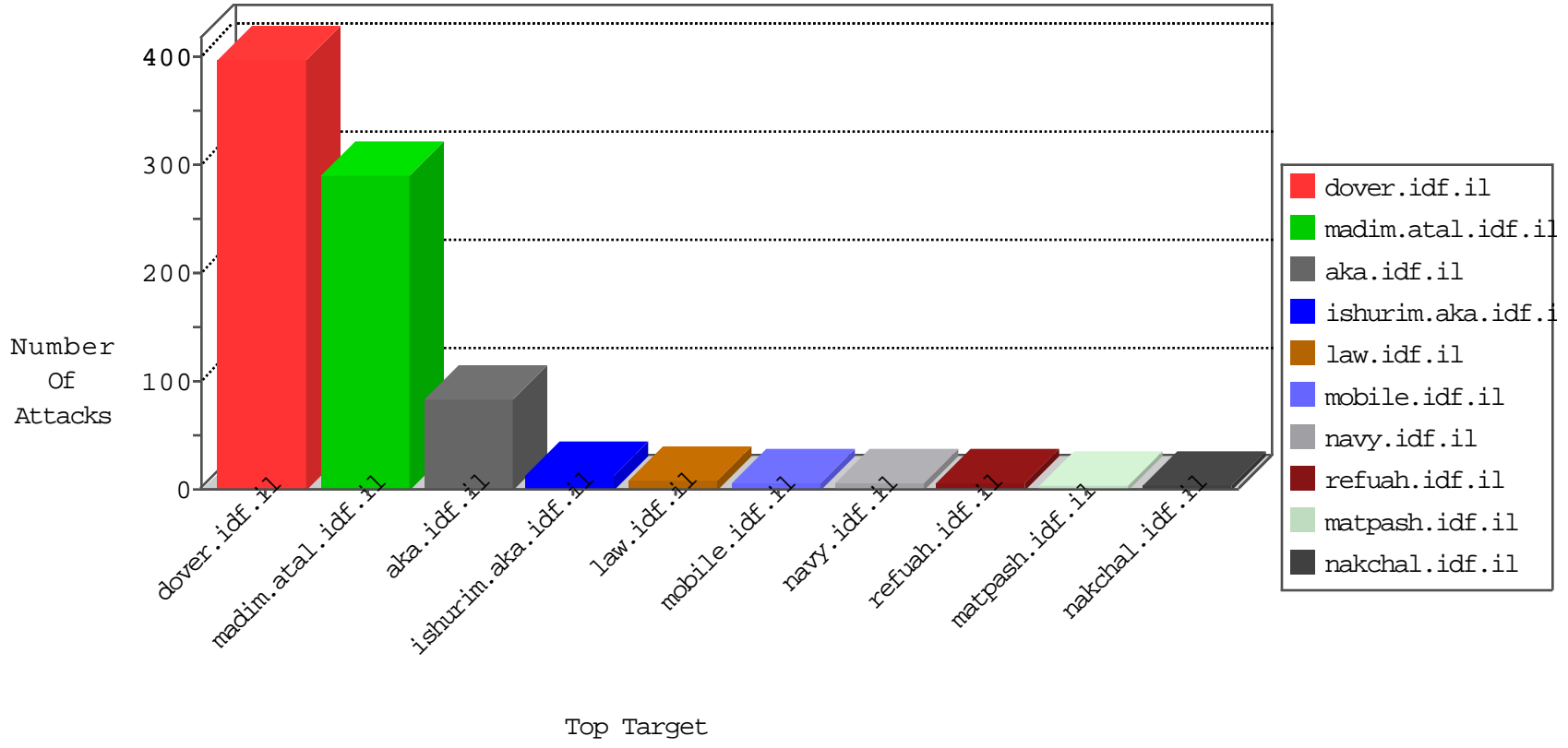
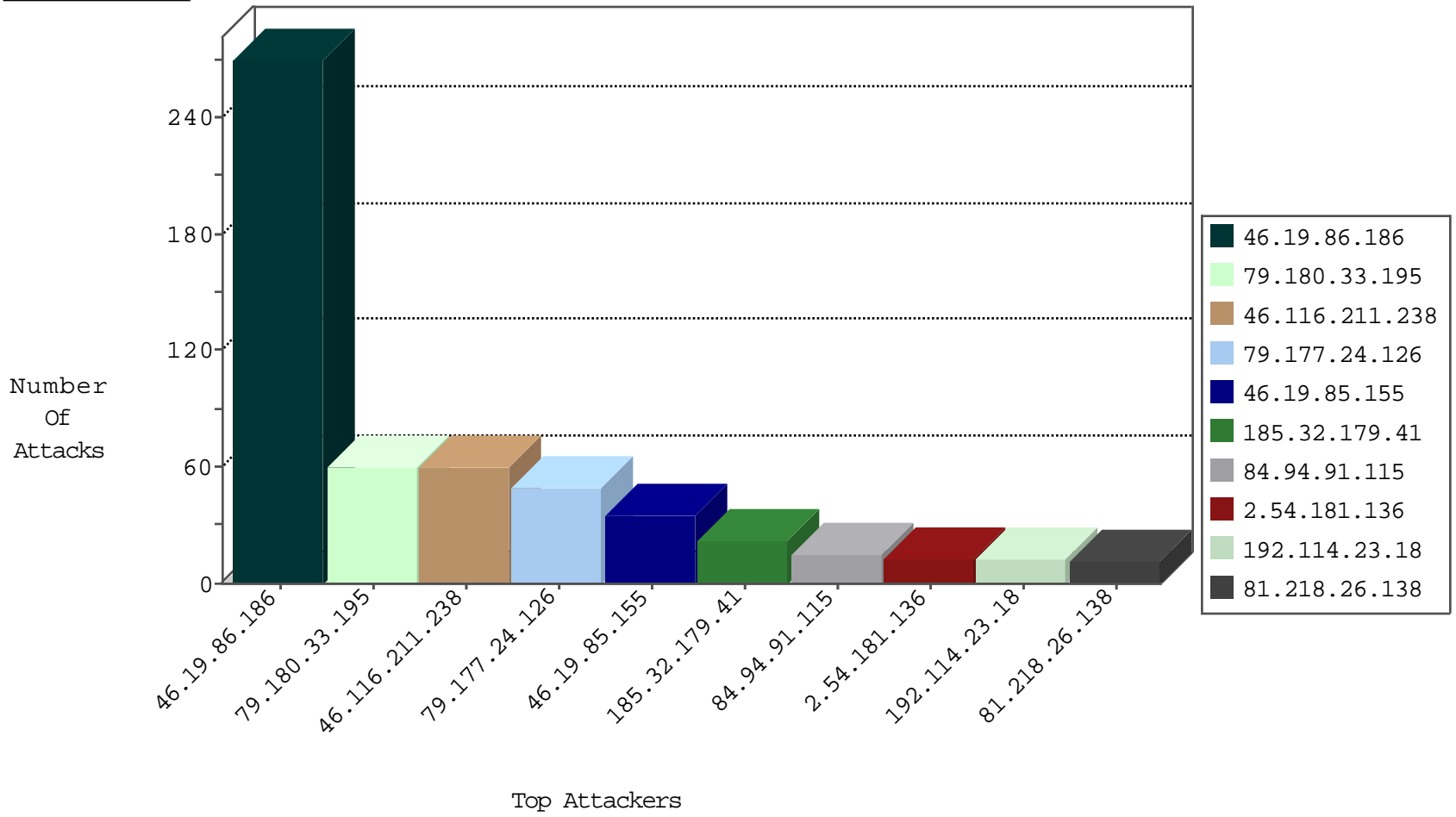




Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3090
66.249.67.34	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1355
149.78.235.223	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	909
109.253.135.42	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	117
109.253.146.136	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	84
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	43
5.144.60.38	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37
2.54.181.136	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	27
89.138.87.210	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
85.250.207.234	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
89.138.80.179	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
212.199.250.22	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
194.56.215.66	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
199.203.158.106	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
95.86.82.169	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
82.80.16.212	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
91.240.80.21	Lebanon	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
87.69.37.129	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
5.29.250.5	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.66.150.184	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
84.228.38.87	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
37.26.148.244	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
149.88.79.41	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
93.172.152.5	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
87.69.92.239	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
5.144.50.37	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.25.84.200	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.235.98.152	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.85.163	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
2.54.43.248	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
180.227.176.121	Korea, Republic of	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
87.69.134.141	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
212.179.28.34	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
89.139.49.143	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
87.68.222.130	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.19.85.210	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
103.18.168.63	India	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
87.69.206.198	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.135.131	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.46	e.chimch.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
212.179.46.20	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.144.121	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.66	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.240	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.147.167	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.175.12	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
217.194.202.19	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
109.253.132.240	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.66	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.162	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
5.102.254.199	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
221.180.149.120	China	147.237.77.235	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
46.116.211.238	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	60
79.180.33.195	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	60
79.177.24.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	49
46.19.85.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
192.114.23.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
81.218.26.138	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
148.177.129.213	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
37.142.173.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
2.54.148.32	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
5.29.202.63	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
37.142.255.85	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
46.19.86.69	Israel	147.237.76.31	nakchal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.246.130.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.177.150.59	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.182.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
93.173.233.142	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.180.52.188	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
5.144.60.38	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.253.143.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
77.127.149.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
178.197.235.93	Switzerland	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.63.223	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
88.49.245.10	Italy	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.183.167.16	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.86.184	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
194.90.200.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.65.127.53	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.101	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
188.120.148.223	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
15.219.153.83	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
85.65.168.241	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
212.199.66.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
157.55.39.58	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
87.68.214.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
192.241.245.200	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
84.228.50.253	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
212.235.98.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
176.12.138.9	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
2.54.18.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
87.68.246.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
193.169.70.108	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
85.65.11.172	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
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	270
185.32.179.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	22
2.54.128.30	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	4
194.114.146.227	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	3
213.8.52.148	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
176.12.138.145	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
109.253.149.193	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
81.218.171.217	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
178.197.235.93	Switzerland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	2
46.19.85.219	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.12.141.62	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.12.141.62	Block	2
2.54.10.24	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
149.78.1.138	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
217.194.196.5	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
79.182.22.220	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.131	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
212.25.102.63	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.25.102.63	Block	2
46.19.85.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.94.174.211	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
81.218.48.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.65	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
188.138.17.205	France	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/	Block	1
85.65.127.53	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to ww.logistics.atal.idf.il/size100x0/sip_storage	Block	1
84.94.91.115	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.85.126	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.94.91.115	Israel	147.237.72.167	ishurim.aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
213.151.37.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
89.138.44.119	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Unknown HTTP Request Method quit in URL	Block	1
176.12.147.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/loginx@x@x.aspx	Block	1
84.108.209.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
52.6.31.228	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-7152-he/	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/eng	Block	1
157.55.39.8	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.94.91.115	Israel	147.237.72.167	ishurim.aka.idf.il	Malformed HTTP Header Line 2	Block	1
212.179.185.90	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.66.122.67	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
85.65.206.133	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
84.94.91.115	Israel	147.237.72.167	ishurim.aka.idf.il	Unknown HTTP Request Method Å£[[#27]]Å^[[#5]]Å?Å'.ÅµÅ.. UÅ.Å½[[#2]]ÅŠzy[[#16]]`9Å"[[#23]]/0]Å?Å©	Block	1
46.19.85.195	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
176.12.141.62	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
84.94.91.115	Israel	147.237.72.167	ishurim.aka.idf.il	Illegal Byte Code Character in Method Å£[[#27]]Å^[[#5]]Å?Å'.ÅµÅ.. UÅ.Å½[[#2]]ÅŠzy[[#16]]`9Å"[[#23]]/0]Å?Å©	Block	1
216.223.27.27	United States	147.237.76.42	refuah.idf.il	URL is Above Root Directory www.refua.atal.idf.il/./images/shared/home.png	Block	1
147.236.31.224	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
91.197.103.1	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/scripts/css3pie.htc	Block	1
79.180.12.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/iaf.org.il	Block	1
54.89.38.190	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1