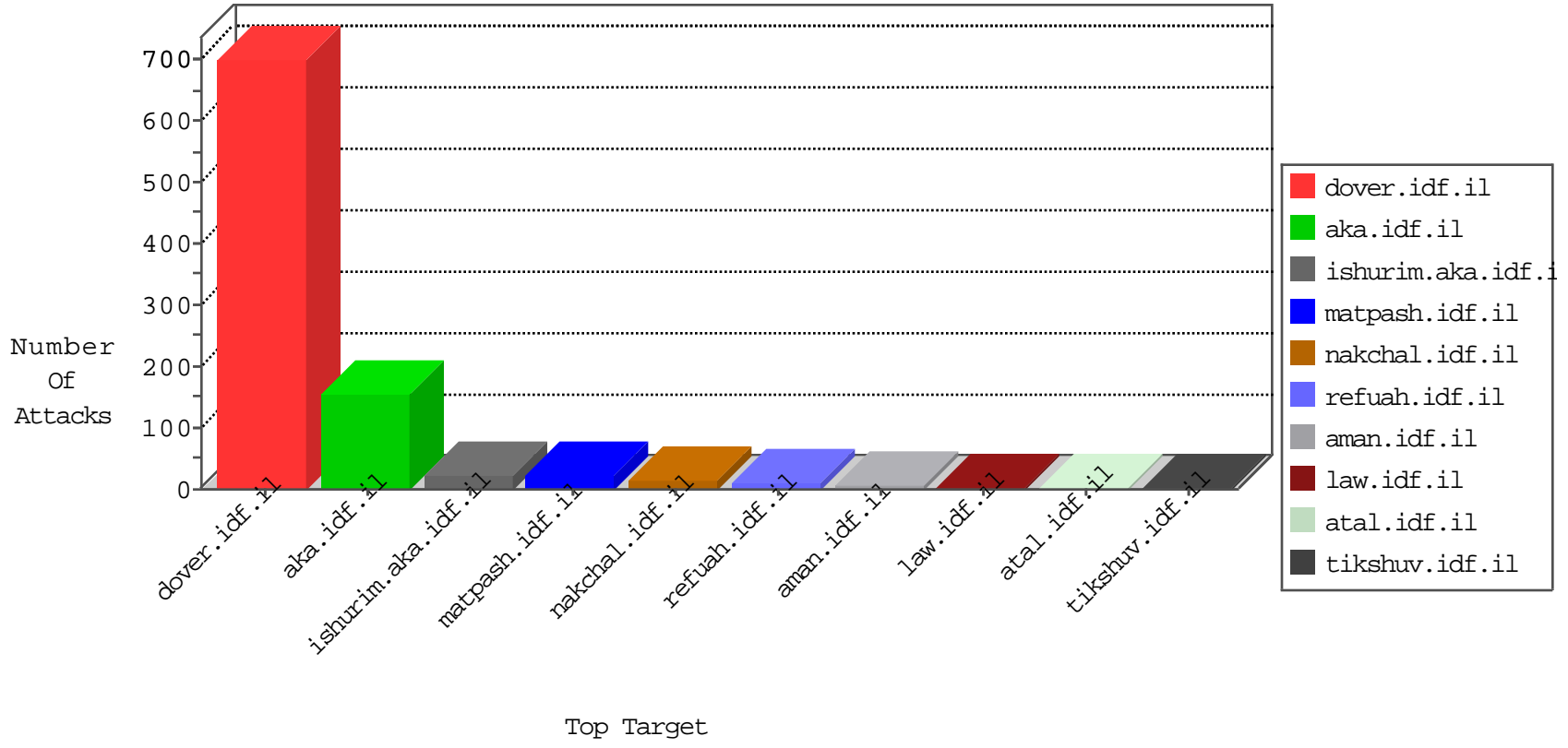
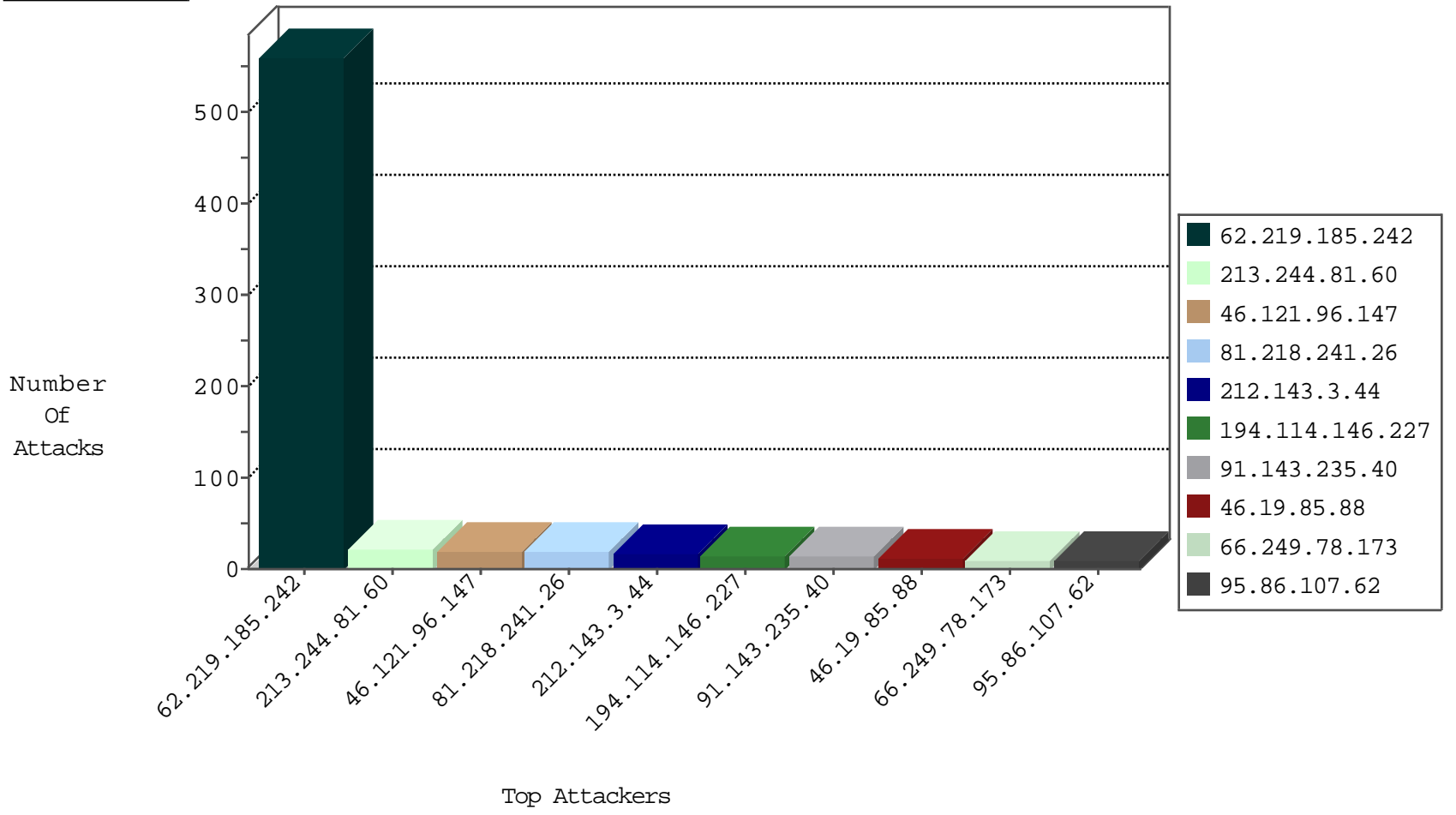




Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	178
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	140
46.121.96.147	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	130
2.54.155.179	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	72
62.219.185.242	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10
37.142.54.109	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
77.125.35.231	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
134.147.203.115	Germany	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	2
134.147.203.115	Germany	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	2
82.102.141.251	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
162.221.206.214	Canada	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
62.219.160.145	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
194.114.146.227	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	14
85.25.103.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.234	halag.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
71.6.165.200	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
79.177.100.170	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
62.90.35.34	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
66.240.236.119	United States	147.237.0.15	kosher-kravi.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	3
109.160.141.9	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
207.232.36.210	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
31.168.195.184	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.138.219	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
116.121.137.2	Korea, Republic of	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
116.121.137.2	Korea, Republic of	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
85.65.6.129	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.153.48	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.185.242	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
218.6.132.45	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.65	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
1.93.24.206	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
116.121.137.2	Korea, Republic of	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
116.121.137.2	Korea, Republic of	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
109.186.18.142	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.217.152	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.94.214.50	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
78.185.95.31	Turkey	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
62.219.185.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	550
213.244.81.60	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	22
91.143.235.40	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
109.253.145.212	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.88	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
46.19.85.88	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
185.32.179.209	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
189.40.89.125	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
2.54.165.252	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.26.148.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.4	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.179.61.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.83	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.235.2.37	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
2.54.181.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
85.250.251.118	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.246.133.54	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
195.200.205.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
82.166.20.41	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
62.219.139.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.52.46.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.109.127.144	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.143.99.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.160.151.153	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.74.107.118	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.52.47.177	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.116.247.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
2.52.47.177	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
87.69.133.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
62.0.197.25	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
37.26.147.137	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
162.243.222.48	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
2.54.32.165	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
201.231.167.194	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
37.26.147.230	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
176.2.1.227	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
82.213.48.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
212.25.84.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
94.230.86.237	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.86.231	Israel	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
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	16
95.86.107.62	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/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	9
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	5
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	5
91.220.22.153	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	5
79.178.153.192	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
87.68.219.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
93.172.169.104	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	4
185.32.179.209	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
80.246.140.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
84.108.49.224	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.253.140.111	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
62.128.48.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.253.133.140	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	2
109.66.33.180	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	2
109.64.108.40	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
89.242.81.18	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	2
37.59.43.170	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
80.246.138.176	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
213.8.99.123	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
37.142.249.217	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
109.64.19.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationsservice.aspx/getuserdetails	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1600-14954-he/dover.aspx	Block	1
89.138.243.237	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
66.249.67.36	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/faq.aspx	Block	1
46.19.86.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
149.78.147.129	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
31.44.143.38	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0207-3.stm	Block	1
212.199.106.194	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19484-he/idfgdover.aspx	Block	1
176.12.147.104	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
94.159.160.110	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
62.219.166.43	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
85.65.236.87	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
79.180.143.184	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
213.8.99.123	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1
46.19.85.81	Israel	147.237.76.42	refuah.idf.il	Distributed Abnormally Long Request	Block	1
109.253.140.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.87	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/sip_storage/files/5/915.pdf full version in hebrew	Block	1
89.145.95.2	United Kingdom	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.39	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/mobile/	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
46.117.134.139	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
149.78.147.129	United States	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
212.199.224.24	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.199.224.24	Block	1
37.26.147.226	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/rabanut/webresource.axd	Block	1