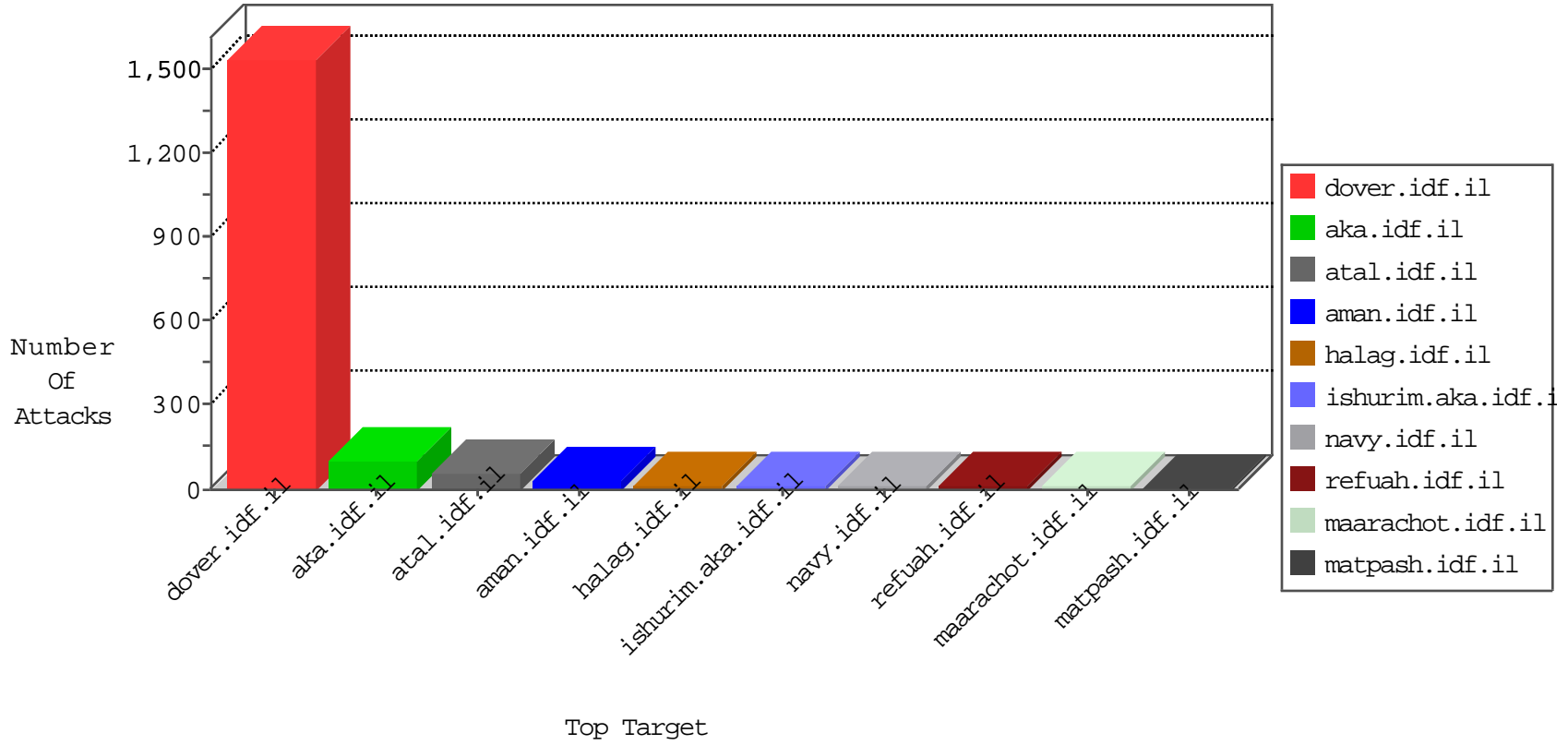
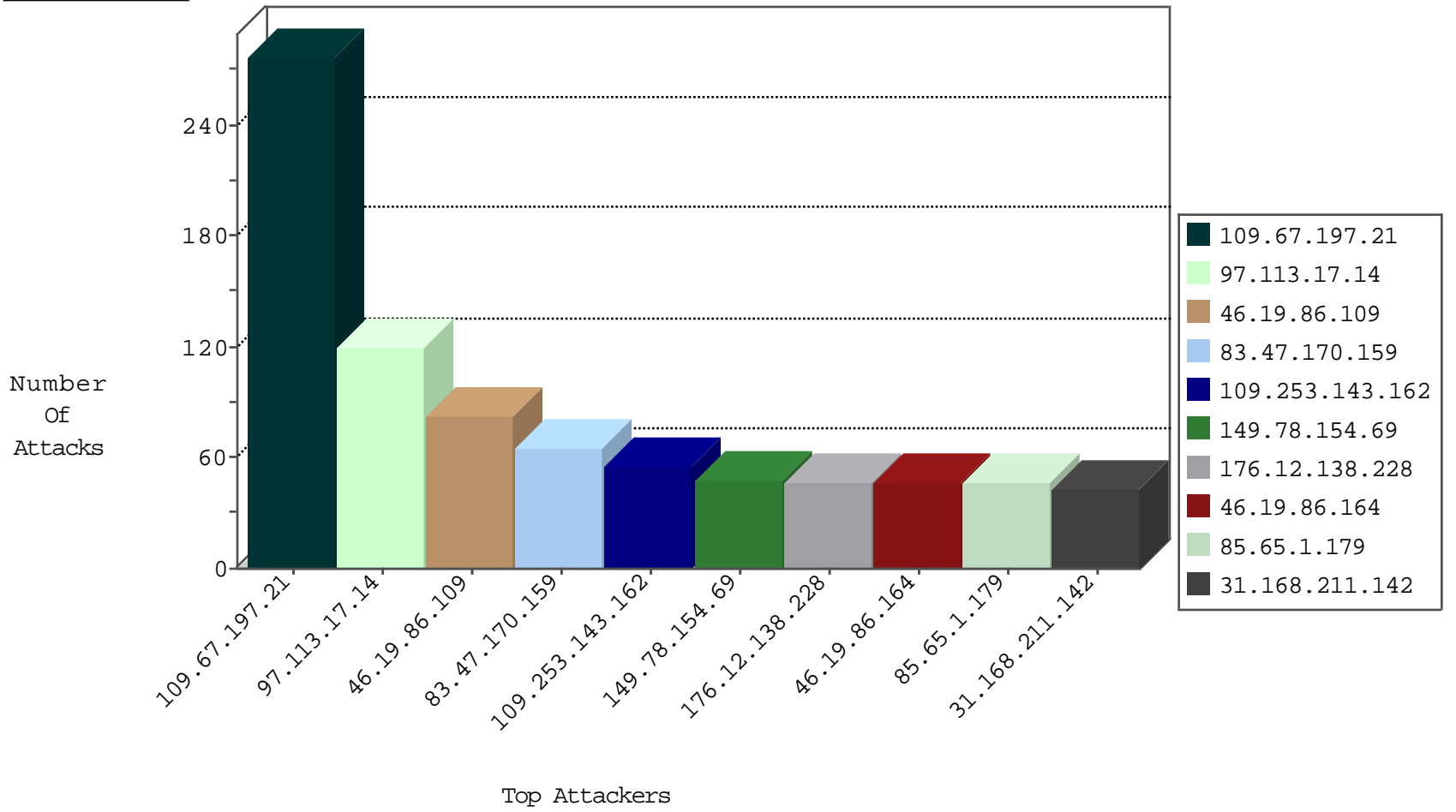


Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.152	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3291
149.78.95.161	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	336
89.139.37.84	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	163
185.32.178.12	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	102
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	8
2.54.30.80	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	3
82.102.141.248	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
5.108.128.103	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
89.139.26.130	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
192.117.186.250	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
31.168.211.142	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
71.6.135.131	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	2
198.20.70.114	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.167	ishurim.aka.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
71.6.165.200	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	1
188.138.9.50	Germany	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.16	my-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	7
66.249.93.168	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
41.45.44.236	Egypt	147.237.77.234	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
197.211.224.17	Zimbabwe	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
31.210.186.143	Israel	147.237.72.167	ishurim.aka.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
162.248.143.132	Canada	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 3072	1
218.77.79.43	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
197.211.224.17	Zimbabwe	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
78.129.148.77	United Kingdom	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
197.211.224.17	Zimbabwe	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
197.211.224.17	Zimbabwe	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
197.211.224.17	Zimbabwe	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
60.18.162.244	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
197.211.224.17	Zimbabwe	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
41.45.44.236	Egypt	147.237.77.243	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
197.211.224.17	Zimbabwe	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
41.45.44.236	Egypt	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
91.238.134.92	Poland	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
197.211.224.17	Zimbabwe	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
78.129.148.77	United Kingdom	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
197.211.224.17	Zimbabwe	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
197.211.224.17	Zimbabwe	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
197.211.224.17	Zimbabwe	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
60.18.162.244	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
197.211.224.17	Zimbabwe	147.237.76.30	hinush.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
109.67.197.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	277
97.113.17.14	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	120
46.19.86.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	82
83.47.170.159	Spain	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
109.253.143.162	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	55
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
176.12.138.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
46.19.86.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
85.65.1.179	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	46
166.137.246.59	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
31.168.211.142	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	37
89.139.179.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
46.19.85.174	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
46.117.123.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
62.24.252.133	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
46.19.85.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
91.135.102.181	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
38.111.147.86	United States	147.237.72.166	aka.idf.il		drop	drop	16
37.26.147.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
93.186.16.213	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
176.12.151.15	Israel	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
46.19.86.215	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
94.230.86.218	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	12
31.210.186.218	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	10
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
32.213.132.193	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
79.181.151.214	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
37.142.119.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
77.69.213.121	Bahrain	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
80.246.130.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.19.85.6	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
68.180.229.51	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
94.230.86.218	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	6
93.186.16.211	South Africa	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
84.108.218.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
31.210.186.143	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
79.178.147.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
2.121.29.171	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
67.80.31.21	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
132.74.244.127	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	6
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
84.111.233.26	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
93.172.131.75	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.137	United States	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
157.55.39.32	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.64.225	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.225	Block	2
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18617-he/kkkkkkkk=8163acf7kkkkkkk_8163acf7	Block	1
66.249.78.161	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.78.161	Block	1
66.249.64.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
93.172.26.175	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/gaash/pics.stm	Block	1
66.249.65.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/templates/sendtofriend/sendtofriend.aspx	Block	1
157.55.39.151	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
66.249.64.209	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
2.54.141.195	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
84.108.34.169	Israel	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
180.76.4.147	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1440-he/refuah.aspx	Block	1
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1537-8800-he/atal.aspx	Block	1
64.251.27.99	United States	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/./shared/usercontrols/headerupper/	Block	1
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Unknown Parameter list in www.aka.idf.il/sites/skira/default.asp	None	1
66.249.64.220	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/iturim/asp/iturimpages.asp	Block	1
31.44.139.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/default.asp	Block	1
185.32.178.110	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/modules/forums/forum.aspx	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	1
94.102.53.195	Netherlands	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/includes/templates/error.tpl	Block	1
66.249.64.187	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/	Block	1
79.176.36.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
157.55.39.191	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/search.asp	Block	1
66.249.73.213	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.73.213	Block	1
31.168.211.142	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
87.69.12.230	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
68.180.229.27	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1234-he/atal.aspx	Block	1
188.120.148.240	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.247	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/haredim/webresource.axd	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
109.253.158.222	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.64.204	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
79.179.36.37	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-10021-en	Block	1
66.249.73.213	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1881	Block	1
157.55.39.32	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
66.249.64.230	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip.storage/files/4/	Block	1