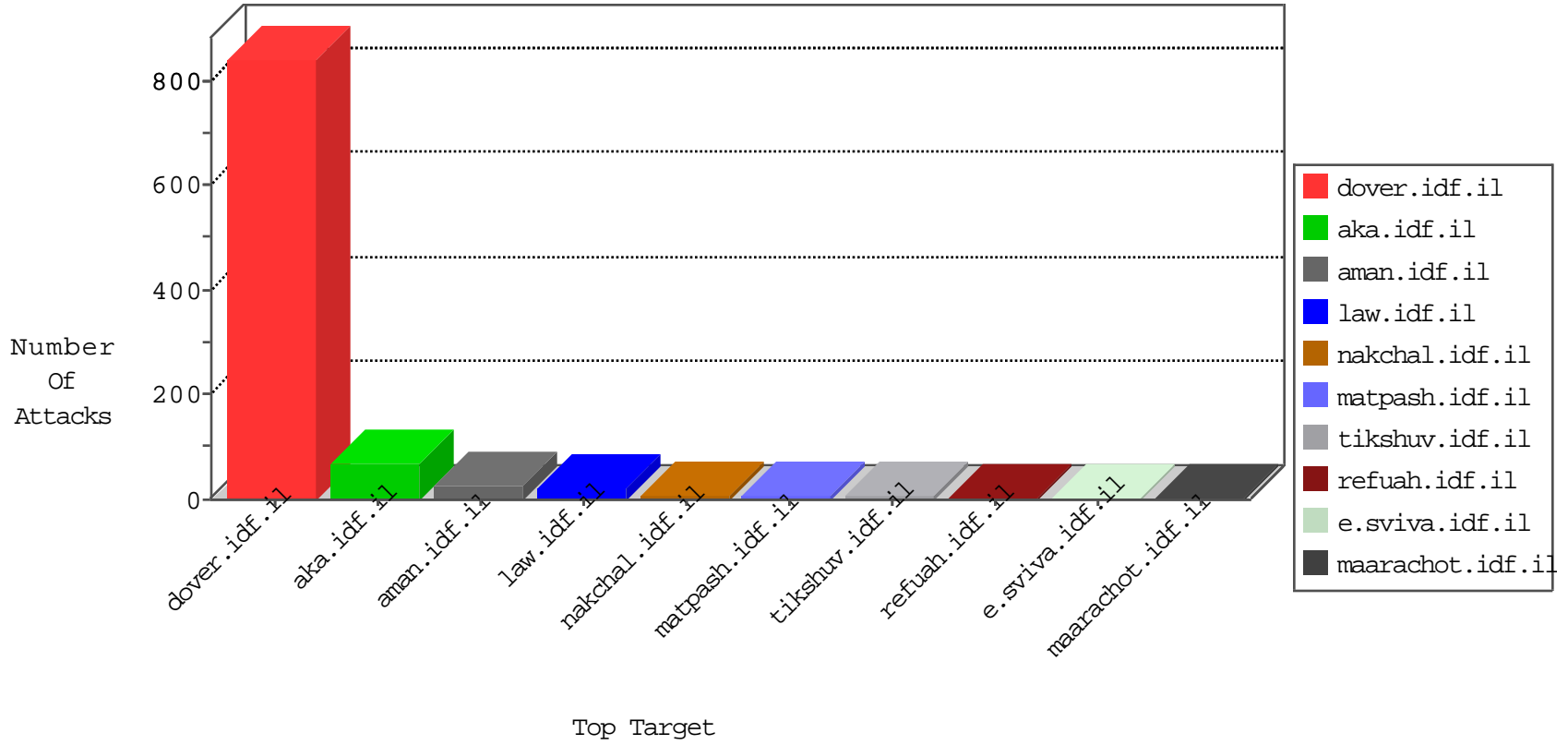
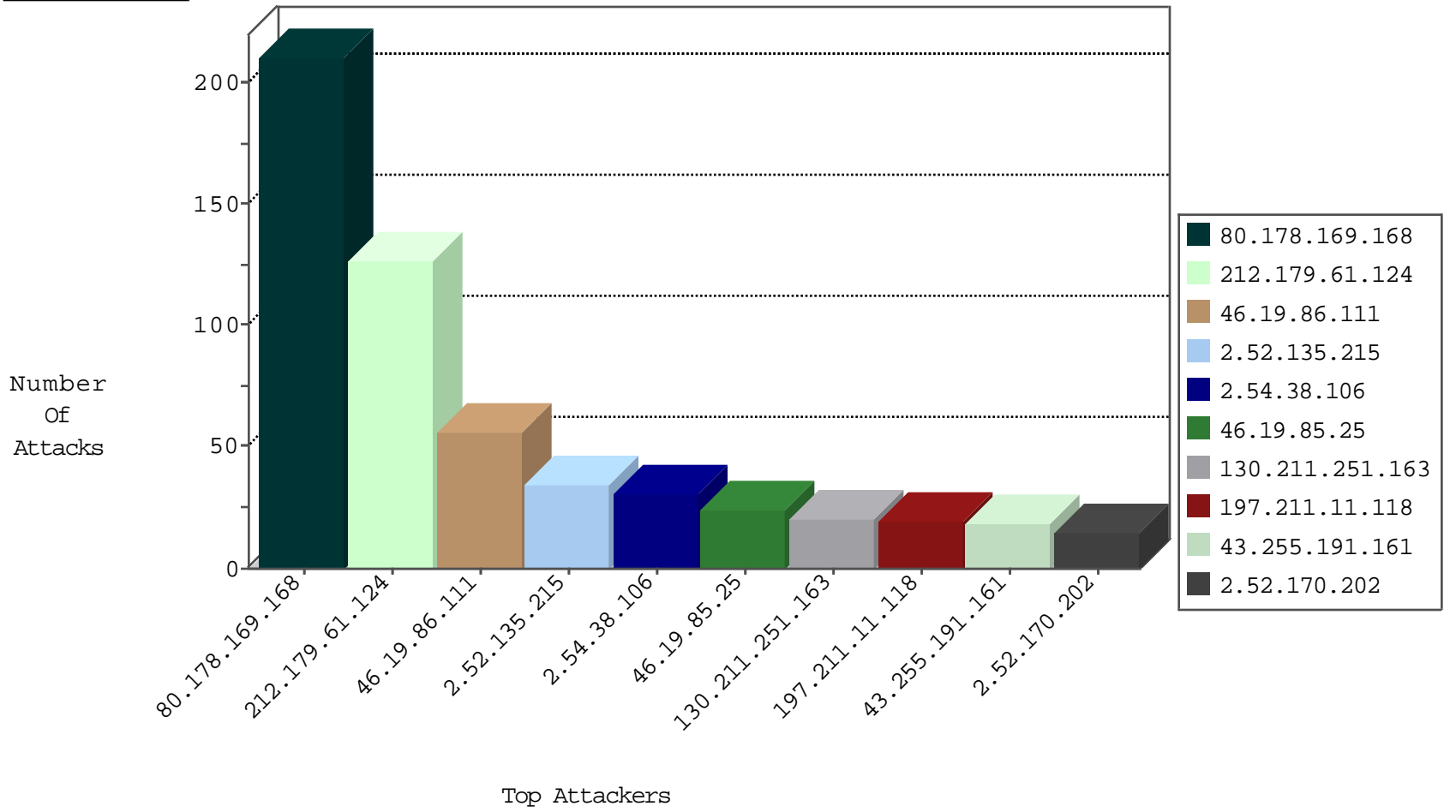




Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
46.19.85.25	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	128
93.173.16.131	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	106
109.65.144.233	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	83
212.179.61.124	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	66
109.160.241.178	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
2.52.15.160	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
79.181.6.145	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
141.138.156.16	France	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
195.37.190.86	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
130.211.251.163		147.237.77.74	law.idf.il	13375: HTTP: Joomla Component JCE BOT for JCE	Block	10
130.211.251.163		147.237.77.74	law.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	10
109.64.103.88	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
198.20.70.114	United States	147.237.77.205	prisha.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
84.111.155.58	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.234	halag.idf.il	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	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.226	www.chamatz.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
66.240.192.138	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.148	ggcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
79.178.203.124	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
84.109.114.190	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.170	maarachot.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	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1

## Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
79.176.37.81	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	4
66.249.73.217	United States	147.237.72.166	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	3
173.252.121.115	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.161	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
218.24.113.2	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.161	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.161	Japan	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
5.196.147.122	Germany	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.161	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	United States	147.237.77.170	maarachot.idf.il	ET DROP Dshield Block Listed Source	1
43.255.191.161	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
80.178.169.168	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	211
212.179.61.124	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	124
46.19.86.111	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	56
2.52.135.215	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	34
2.54.38.106	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
46.19.85.25	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
197.211.11.118	Kenya	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
2.52.170.202	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
201.141.206.164	Mexico	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
176.228.50.222	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	13
176.12.138.45	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.144.14	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
79.182.98.234	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
176.12.146.60	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
194.90.209.187	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
212.179.42.225	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	9
217.132.66.147	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
2.54.50.35	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
52.16.5.197	United States	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
41.33.232.65	Egypt	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
132.64.30.46	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
207.46.13.52	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
77.248.22.227	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
79.180.140.36	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	5
46.19.86.143	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
77.125.145.131	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
194.142.172.55	Finland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
212.143.3.44	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
87.68.154.173	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
93.173.16.211	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
37.26.146.221	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
213.57.39.72	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
91.135.102.165	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
46.117.69.175	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
93.172.34.126	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
95.86.116.207	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
2.52.56.82	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
62.219.119.35	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
84.108.144.240	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
176.12.136.40	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
46.117.12.185	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
87.68.41.208	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
176.12.150.130	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
46.19.85.218	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
109.67.37.176	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
212.76.127.111	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2

**Top Attackers In WAF**

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	7
95.86.113.239	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	6
79.179.102.178	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
95.86.70.213	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	4
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	3
185.32.177.70	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
213.57.187.251	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.117.16.143	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
176.12.143.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.64.103.88	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
77.127.54.106	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	2
77.127.219.208	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
79.183.101.24	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
162.243.198.188	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 162.243.198.188	Block	2
79.177.96.183	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1403	Block	2
80.246.138.121	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
31.168.68.51	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q861 in www.aka.idf.il/main/gyius/login.aspx	None	1
77.126.30.188	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
141.212.122.82	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
66.249.73.217	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
93.173.229.137	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//https://www.idf.il/	Block	1
79.177.110.53	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https://www.aka.idf.il/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0326-2.stm	Block	1
66.249.65.58	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
84.111.33.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottonnavigaton.asp	Block	1
37.142.118.48	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https://www.aka.idf.il/	Block	1
216.223.27.27	United States	147.237.76.30	himush.idf.il	URL is Above Root Directory www.chimush.atal.idf.il/.../images/shared/home.png	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/family	Block	1
46.117.71.58	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.59.197.235	Kazakstan	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method COOK in URL www.cogat.idf.il/896-en/idfg.aspx	Block	1
68.180.229.36	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//894-he/refuah.aspx	Block	1
180.76.4.171	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.65.175	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
109.253.134.35	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.228.171.157	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
37.142.204.132	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.142.204.132	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chanatz/klali/default.asp	None	1
46.121.247.55	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https://www.aka.idf.il/	Block	1
69.58.178.58	United States	147.237.76.31	nakchal.idf.il	Suspicious Response Code	Block	1
115.151.64.66	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-10868-en/dover.aspx/trackback/	Block	1
66.249.65.178	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-6294-he/patzar.aspx	Block	1
84.228.216.22	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.142.204.132	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/x'x'x'x'x'	Block	1
79.176.37.81	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/ordnance/ordnance.stm	Block	1
61.135.190.68	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
95.86.70.213	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
80.246.136.110	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
69.58.178.58	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/.../shared/usercontrols/headerupper/	Block	1