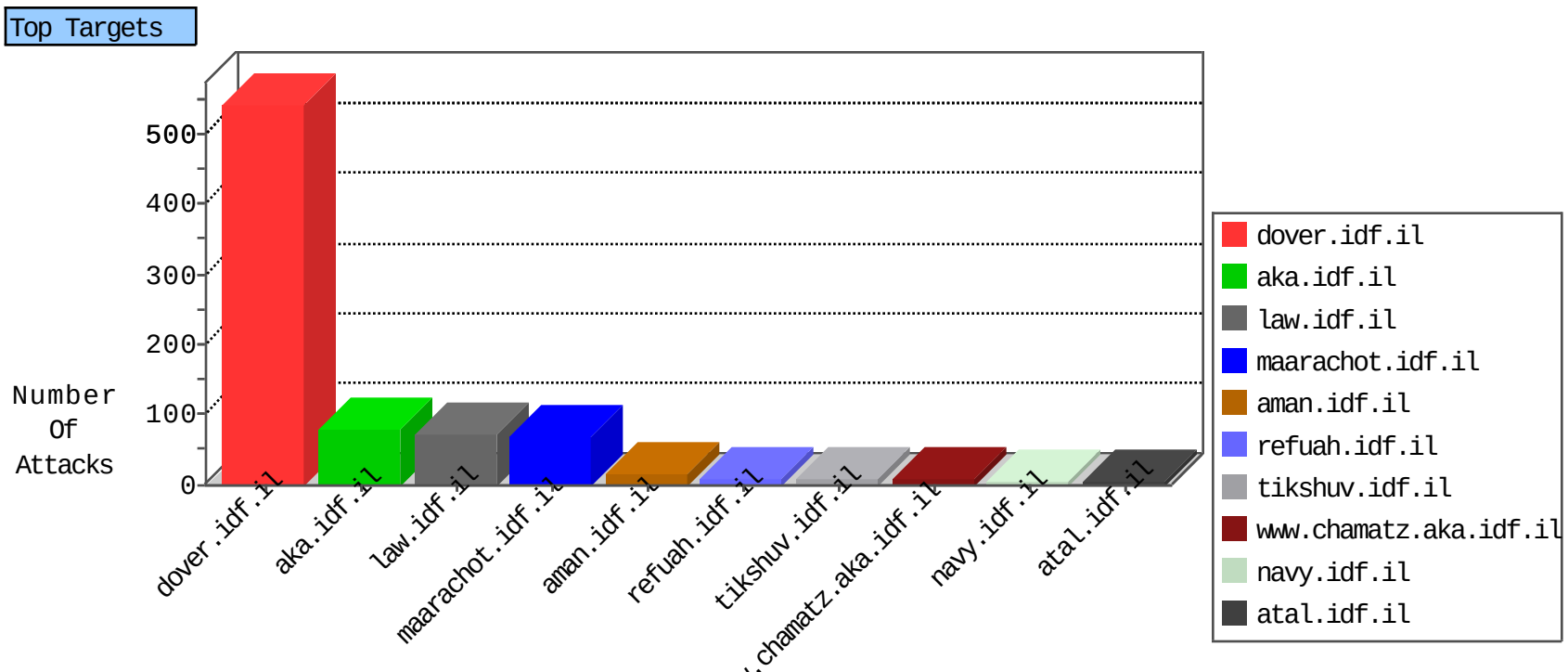
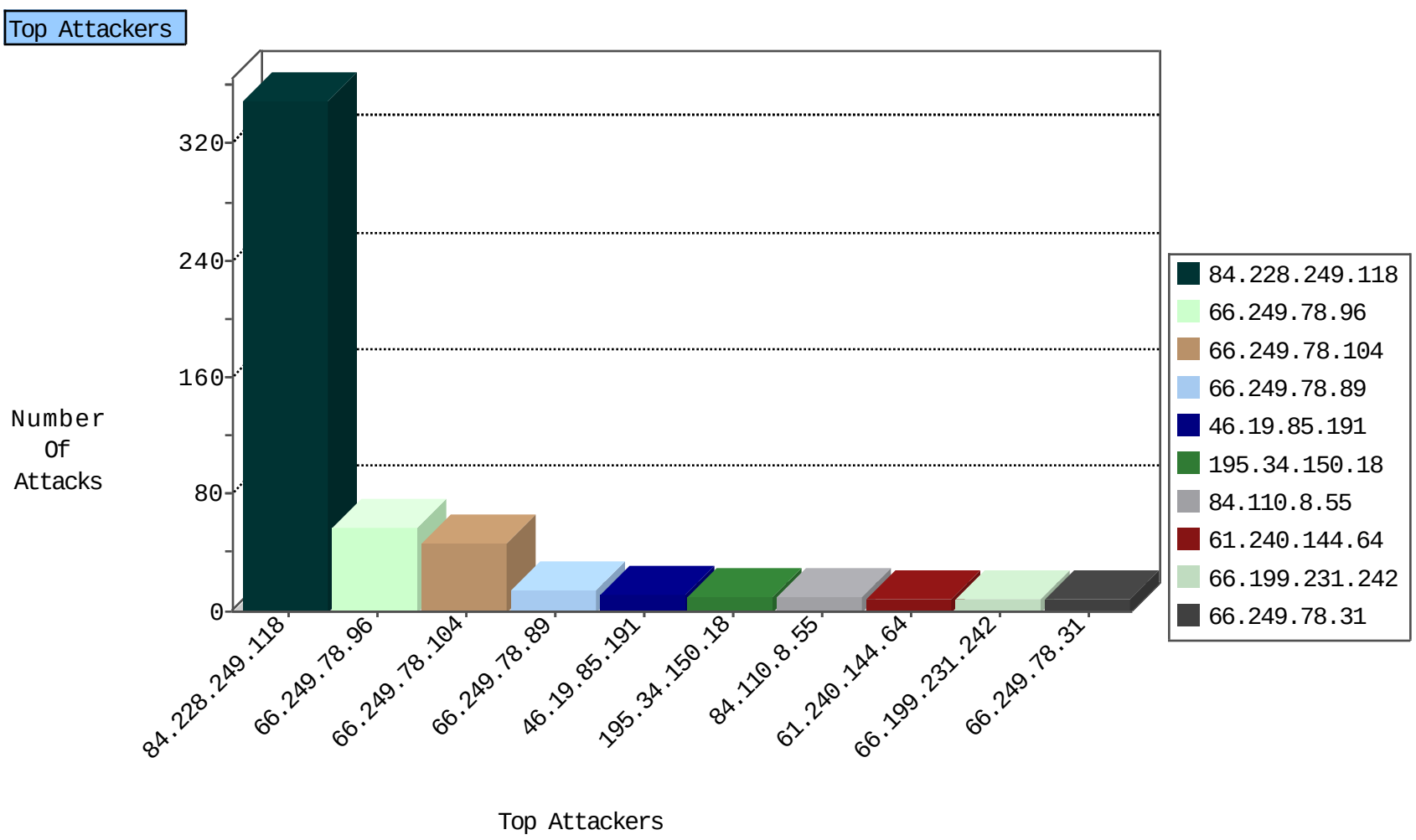
04-26-2015-21:03:01 to 04-26-2015-22:03:01

IDF Under Attack
04-26-2015-21:03:01

Top Targets



Top Attackers



04-26-2015-21:03:01 to 04-26-2015-22:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.96	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	5418
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3979
66.249.78.31	Israel	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	3261
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	2236
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1872
220.181.108.84	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	393
84.110.8.55	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	95
46.19.85.191	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	45
82.166.181.225	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
66.249.67.39	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	8
79.177.8.129	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	6
66.249.78.11	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	6
5.144.51.85	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
46.19.85.121	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
192.168.1.103		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
212.179.213.178	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
79.183.134.182	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	1
2.54.28.158	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
84.228.198.87	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.120.17.35	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
91.240.80.21	Lebanon	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
114.80.215.201	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

04-26-2015-21:03:01 to 04-26-2015-22:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
71.6.167.142	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
213.57.206.72	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

04-26-2015-21:03:01 to 04-26-2015-22:03:01

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
85.64.3.211	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.180.214.31	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.69.77	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
37.142.157.198	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
61.240.144.64	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
61.175.255.61	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 4096	1
60.18.162.244	China	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.190.60	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
41.35.192.211	Egypt	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
23.254.131.164	United States	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.64	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
23.254.131.164	United States	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
213.210.205.2	Saudi Arabia	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
108.29.0.76	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.64	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
85.65.86.19	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
61.175.255.61	China	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.42	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
43.255.190.60	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
23.254.131.164	United States	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
213.210.205.2	Saudi Arabia	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 3072	1
1.34.90.227	Taiwan	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1

04-26-2015-21:03:01 to 04-26-2015-22:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.228.249.118	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	350
79.178.151.3	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
85.65.74.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
109.67.180.192	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.117.26.50	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
89.139.173.70	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
92.99.171.77	United Arab Emirates	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
108.29.0.76	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
89.138.64.3	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
82.166.247.66	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
93.172.174.203	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.66.3.124	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
181.28.228.44	Argentina	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	alert	3
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
95.86.66.128	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.117.112.55	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.142.227.171	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.246.130.39	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
174.51.4.217	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.52.149.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.180.143.10	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
89.139.173.70	Israel	147.237.72.156	aman.idf.il		drop	drop	2
77.125.134.139	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
176.12.144.74	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.69.48	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.65.74.82	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	2
2.52.183.148	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.181.48.61	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
54.147.176.220	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
66.249.80.67	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
94.159.203.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.183.61.21	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.177.206.189	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.93.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
87.211.90.118	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
72.133.254.59	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
157.55.39.59	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.19.85.162	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
216.223.27.58	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
2.52.44.236	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
188.120.148.222	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
66.249.93.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
207.46.13.95	United States	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
66.199.231.242	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.199.231.242	Block	8
79.177.207.213	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	6
37.26.146.216	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
54.147.176.220	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
46.121.104.248	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
66.249.75.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.75.66	Block	2
84.228.197.89	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
93.172.159.85	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.69.32	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//938-he/refuah.aspx	Block	1
85.64.119.110	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
46.116.209.83	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
212.76.107.19	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
77.237.154.221	Czech Republic	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/- + encodeuri(url) +	Block	1
5.29.41.221	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/relativecontact.aspx	None	1
157.55.39.8	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.173.128.24	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.75.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/kids.stm	Block	1
82.102.136.67	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
213.151.47.137	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
176.228.35.71	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//1518-he/refuah.aspx	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0306-4.stm	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.125	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-8607-he/dover.aspx	Block	1
85.65.74.82	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
79.176.13.8	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.76.109.175	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.160	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
5.29.44.228	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.8	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/klali.aspx	Block	1
109.66.3.124	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/insignia/tags.stm	Block	1
84.108.40.118	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
66.199.231.242	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/info.asp	Block	1
216.223.27.22	United States	147.237.77.74	law.idf.il	URL is Above Root Directory www.law.idf.il/../images/trans.gif	Block	1
46.19.85.136	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
181.28.228.44	Argentina	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//webresource.axd	Block	1
71.246.115.237	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyusgeneral.aspx	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/info.asp	Block	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
85.65.113.183	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
52.1.90.117	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
212.143.3.44	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/main/giyus/general.aspx	Block	1
31.13.100.116	Ireland	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/901-8342-he	Block	1
157.55.39.115	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
149.78.203.14	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1