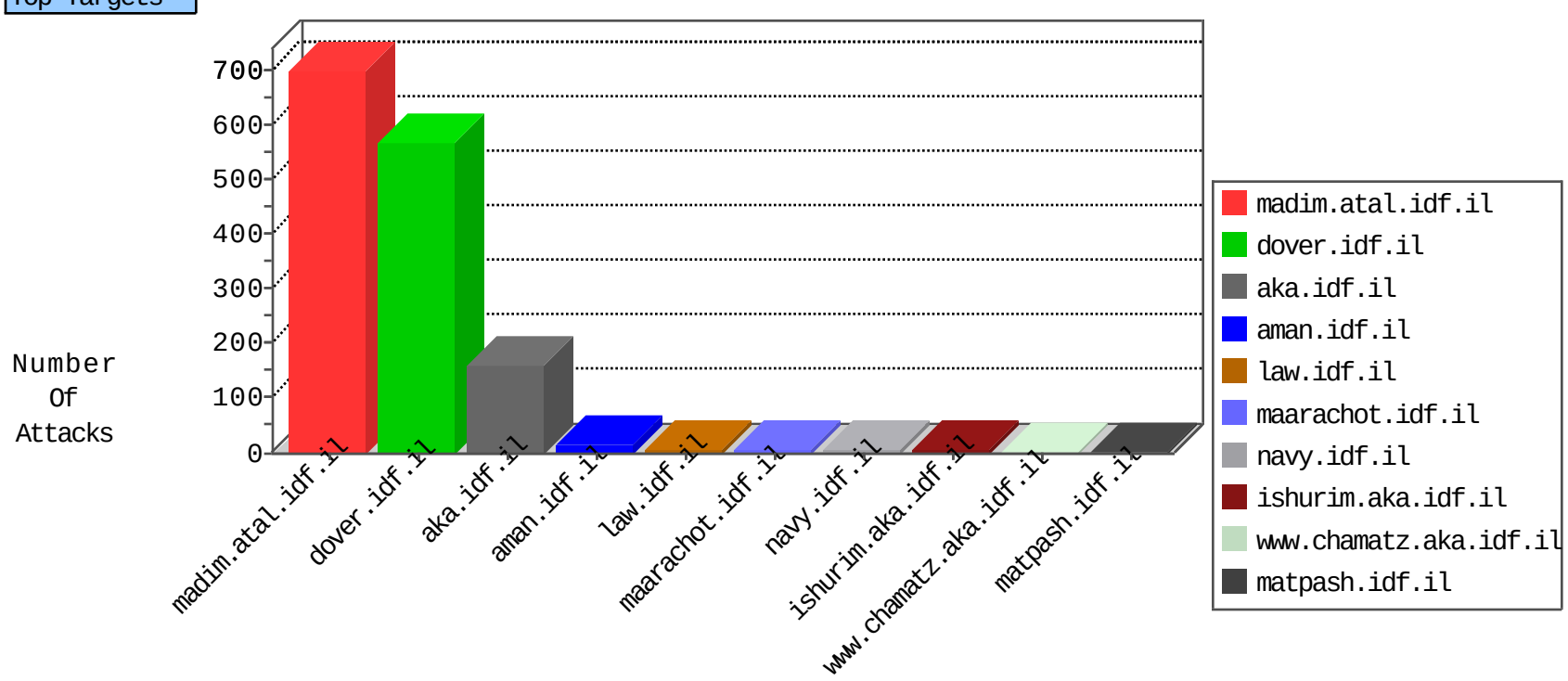
04-26-2015-17:03:04 to 04-26-2015-18:03:04

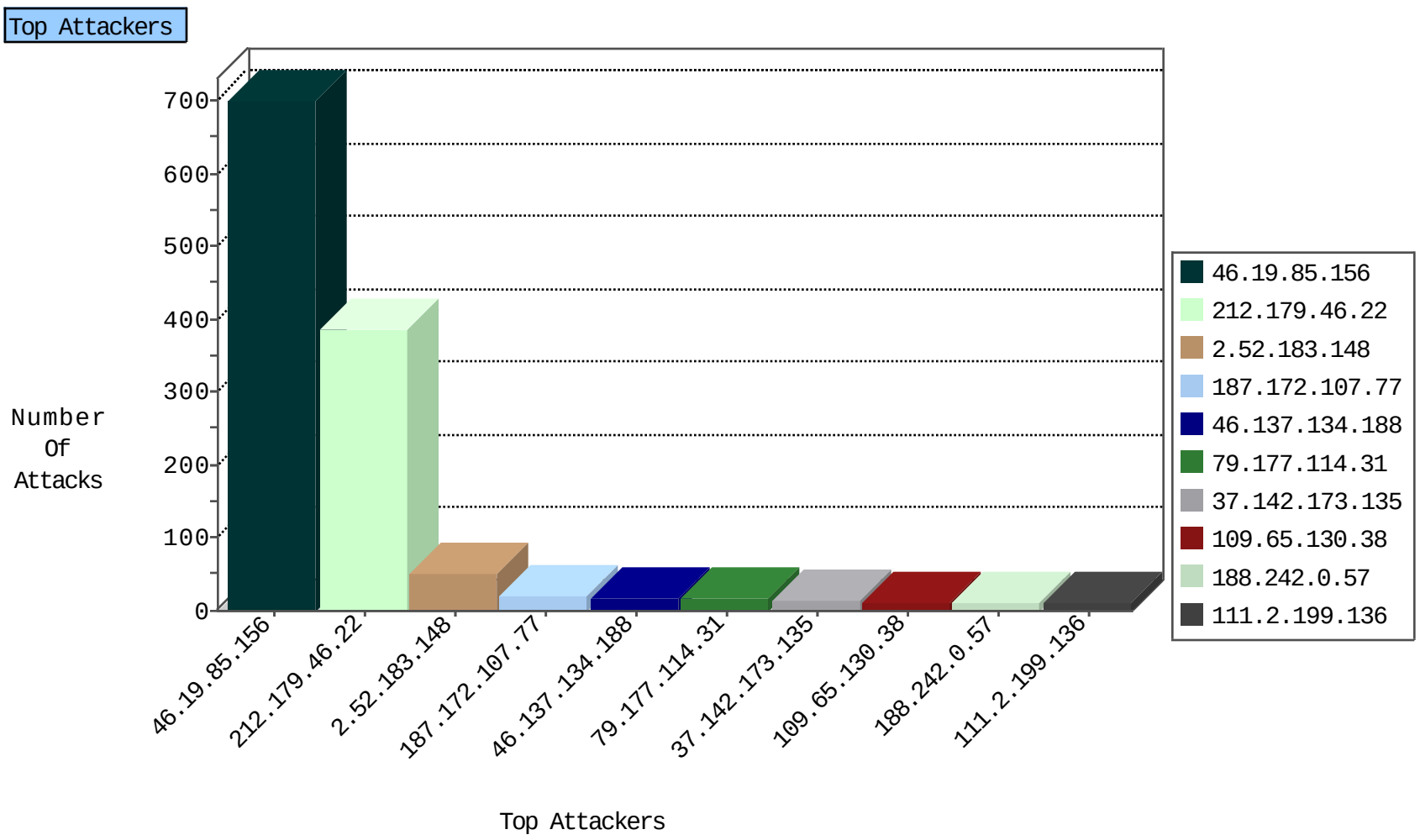
IDF Under Attack
04-26-2015-17:03:04

Top Targets



Top Target

Top Attackers



Top Attackers

04-26-2015-17:03:04 to 04-26-2015-18:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.97	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	926
66.249.78.89	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	374
46.117.80.162	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	6
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1

04-26-2015-17:03:04 to 04-26-2015-18:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	9
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	9
80.246.139.23	Israel	147.237.72.156	aman.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
213.8.242.46	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
66.240.192.138	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.17.242.234	Netherlands	147.237.77.176	matpash.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
66.240.236.119	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.121	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	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
192.114.2.36	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
71.6.165.200	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
197.38.251.3	Egypt	147.237.77.216	dover.idf.il	12618: HTTP: WebCruiser Vulnerability Scanner	Block	1

04-26-2015-17:03:04 to 04-26-2015-18:03:04

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	4
194.90.88.105	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
109.65.120.75	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
188.242.0.57	Russian Federation	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
85.250.157.52	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
188.242.0.57	Russian Federation	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
111.2.199.136	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	United States	147.237.77.19	law-forum.idf.il	ET DROP Dshield Block Listed Source	1
79.178.143.115	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
111.2.199.136	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
111.2.199.136	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
46.116.106.99	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
188.242.0.57	Russian Federation	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
111.2.199.136	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.121	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
188.242.0.57	Russian Federation	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
111.2.199.136	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
23.254.131.164	United States	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
188.242.0.57	Russian Federation	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
109.253.77.199	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
188.242.0.57	Russian Federation	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
109.65.112.13	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
188.242.0.57	Russian Federation	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
84.228.237.150	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
176.58.77.251	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
212.116.172.1	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.168.154	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
111.2.199.136	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
195.154.150.239	France	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 3072	1
66.249.67.157	United States	147.237.72.166	aka.idf.il	ET SCAN NMAP -sA (2)	1
111.2.199.136	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
46.120.62.87	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
111.2.199.136	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.241	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
188.242.0.57	Russian Federation	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
111.2.199.136	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
37.26.147.171	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
188.242.0.57	Russian Federation	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
111.2.199.136	China	147.237.77.61	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
188.242.0.57	Russian Federation	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1

04-26-2015-17:03:04 to 04-26-2015-18:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.46.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	386
2.52.183.148	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
37.142.173.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
176.58.77.251	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
85.65.6.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
79.181.117.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
100.1.96.142	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
62.219.98.31	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.241	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
5.22.129.139	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	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
46.19.85.174	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.199.130.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.49.236	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	2
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
81.218.40.194	Israel	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
46.19.85.181	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.49.236	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid sequence number	Bad TCP sequence	monitor	2
83.244.48.131	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.33.105.106	Palestinian Territory, Occupied	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
212.117.132.139	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
2.54.42.26	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
80.246.130.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
199.16.156.126	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.65.52.65	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.45.46	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.64.126.217	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.26.147.241	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
89.108.159.50	Lebanon	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
37.46.39.192	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
93.172.169.51	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
77.127.238.96	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
94.230.86.145	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
194.90.88.105	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.86.38	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.150	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
80.246.133.228	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.86.141	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
46.19.85.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	700
79.177.114.31	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	16
109.65.130.38	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	11
80.179.143.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
187.172.107.77	Mexico	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	8
187.172.107.77	Mexico	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 187.172.107.77	Block	5
109.64.54.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
2.54.12.167	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	4
5.102.221.15	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
109.160.237.110	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
213.151.52.41	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
95.86.121.176	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	3
5.29.79.241	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
85.65.15.141	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
82.166.148.185	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
77.127.238.96	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	2
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
193.34.56.101	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
89.139.176.236	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.111.210.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.176.158.186	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
187.172.107.77	Mexico	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
77.127.200.19	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/sachar/undefined	Block	2
194.90.116.157	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.127.225.169	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
66.249.67.43	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
109.253.77.199	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
46.19.85.42	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
197.38.251.3	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/homepage.aspx/shared/usercontrols/headerupper/	Block	1
79.181.128.206	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.143.126	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
149.78.194.187	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.95	Block	1
46.120.132.144	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
217.87.111.236	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
187.172.107.77	Mexico	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim//sip_storage/files/2/66102.jpg	Block	1
66.249.69.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1384-11002-he/dover.aspx	Block	1
109.253.136.158	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.65.193.69	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
207.46.13.131	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.151.135	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
79.181.215.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-13725-en/dover.aspx	Block	1
66.199.231.242	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
217.132.93.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
109.64.132.120	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
31.154.12.22	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.109.188.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1