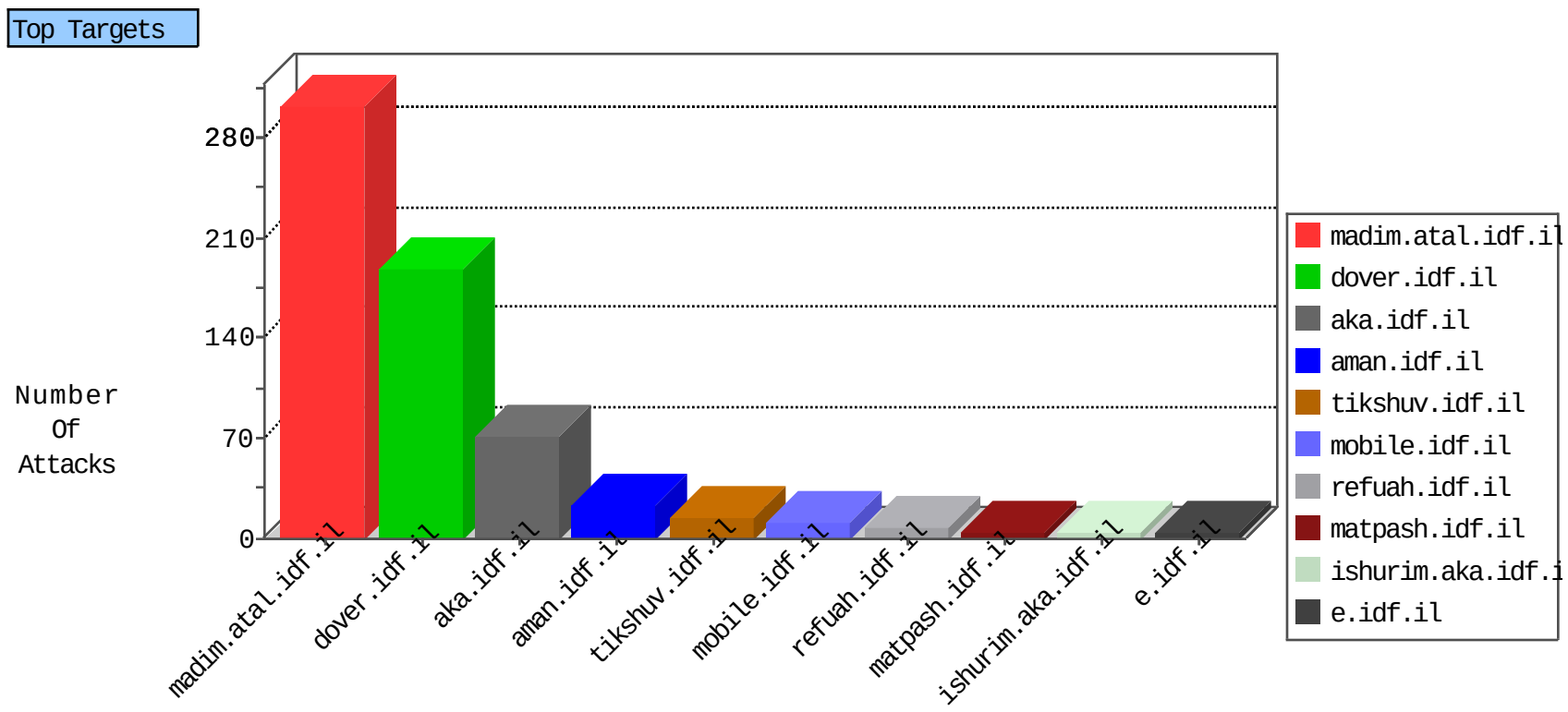
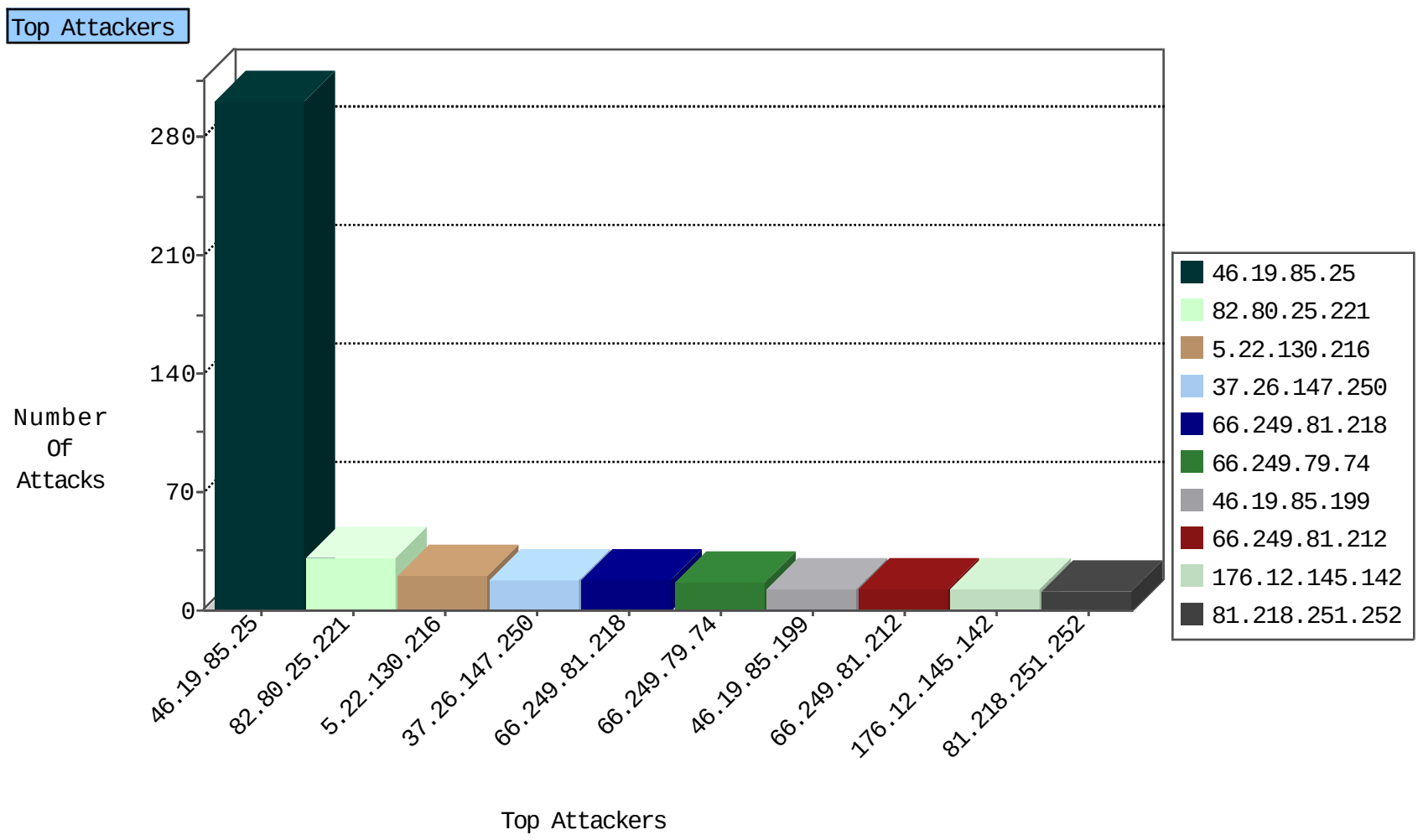
03-27-2015-10:03:08 to 03-27-2015-11:03:08

IDF Under Attack
03-27-2015-10:03:08

Top Targets



Top Attackers



03-27-2015-10:03:08 to 03-27-2015-11:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count

03-27-2015-10:03:08 to 03-27-2015-11:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
81.218.251.252	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	11
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	4
85.25.43.94	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1

03-27-2015-10:03:08 to 03-27-2015-11:03:08

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	31
77.126.137.81	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
84.109.96.215	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
2.54.14.66	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
132.66.10.154	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
80.246.130.173	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
61.160.224.130	China	147.237.77.234	halag.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
211.138.34.58	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.130	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.160.224.130	China	147.237.72.156	aman.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
130.207.203.56	United States	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
31.7.57.198	Switzerland	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
115.231.218.147	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
104.37.103.17		147.237.72.166	aka.idf.il	SERVER-WEBAPP bad HTTP/1.1 request, Potentially worm attack	1
61.160.224.130	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
198.20.69.74	United States	147.237.76.202	e.halag.idf.il	ET DROP Dshield Block Listed Source	1
61.160.224.130	China	147.237.72.217	e.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.160.224.130	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
115.231.218.147	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.60	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
115.231.218.147	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
114.255.149.210	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1

03-27-2015-10:03:08 to 03-27-2015-11:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.81.218	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.79.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
37.26.147.250	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	16
66.249.81.212	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
176.12.145.142	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
5.22.130.216	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	11
5.22.130.216	Israel	147.237.72.156	aman.idf.il	First packet isn't SYN	drop	drop	7
176.12.146.185	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.147.24	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.130.185	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.139.186	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.199	Israel	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	6
176.12.142.58	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.199	Israel	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	6
46.32.208.11	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	5
46.32.208.11	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
109.253.146.169	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
2.52.172.22	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
109.253.145.77	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
207.46.13.112	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
66.249.79.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
46.19.86.4	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
5.22.130.216	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	2
188.165.15.196	France	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
2.52.139.102	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
104.37.103.17		147.237.72.217	e.idf.il	SAM rule	drop	drop	2
46.19.86.84	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
37.26.147.250	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
80.246.139.54	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
46.117.246.52	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.225	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
31.168.96.254	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
108.61.228.169	United States	147.237.76.147	chinuch.aka.idf.il		drop	drop	1
79.182.34.222	Israel	147.237.77.74	law.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.122	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
37.26.148.236	Israel	147.237.72.156	aman.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	1
84.108.157.243	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
184.105.139.84	United States	147.237.0.33	idf.il		drop	drop	1
37.26.147.173	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
80.246.137.202	Israel	147.237.72.167	ishurim.aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	1
46.19.86.204	Israel	147.237.76.31	nakchal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
212.150.200.61	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.49	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
84.109.16.246	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
46.19.86.4	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
185.32.177.148	Israel	147.237.72.167	ishurim.aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	1
109.253.142.142	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
2.52.0.139	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.85.25	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.25	Block	301
213.151.48.4	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
66.249.67.120	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.67.120	Block	4
2.54.140.205	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.140.205	Block	4
2.54.140.205	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	3
66.249.79.66	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	3
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	3
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
104.37.103.17		147.237.72.167	ishurim.aka.idf.i	Multiple Unauthorized URL Access from 104.37.103.17	Block	2
212.76.111.62	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
66.249.79.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/feburary/20.stm	Block	1
213.57.187.83	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/home.aspx	None	1
176.12.149.208	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
104.37.103.17		147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 104.37.103.17	Block	1
80.246.141.165	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.73.217	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.28.130.205	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/rabanut/faq.aspx	None	1
95.130.13.153	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.130.13.153	Block	1
66.249.79.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/april/03a.stm	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18606-en/kkkkkkk=cb7c1679kkkkkkk_cb7c1679	Block	1
46.19.85.119	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
104.37.103.17		147.237.72.166	aka.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
84.108.157.243	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.73.235	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ie-contacts.stm	Block	1
37.26.147.221	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.138.165	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.130.13.153	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
180.76.5.172	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
84.229.33.70	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/default.aspx	None	1
66.249.79.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0113-4.stm	Block	1
207.241.237.228	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.140.141.39	Russian Federation	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
176.12.139.123	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
104.37.103.17		147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
79.179.2.134	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
185.32.179.139	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.201	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	1
109.253.140.116	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
84.229.33.70	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
176.12.144.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.25	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
104.37.103.17		147.237.72.156	aman.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
79.182.196.37	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
66.249.73.201	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/×©×§×• ×¤×™×ª 6	Block	1
2.54.162.71	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/eitan/mesiratmeida/	None	1
85.65.185.40	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/6_s3_	Block	1

03-27-2015-10:03:08 to 03-27-2015-11:03:08