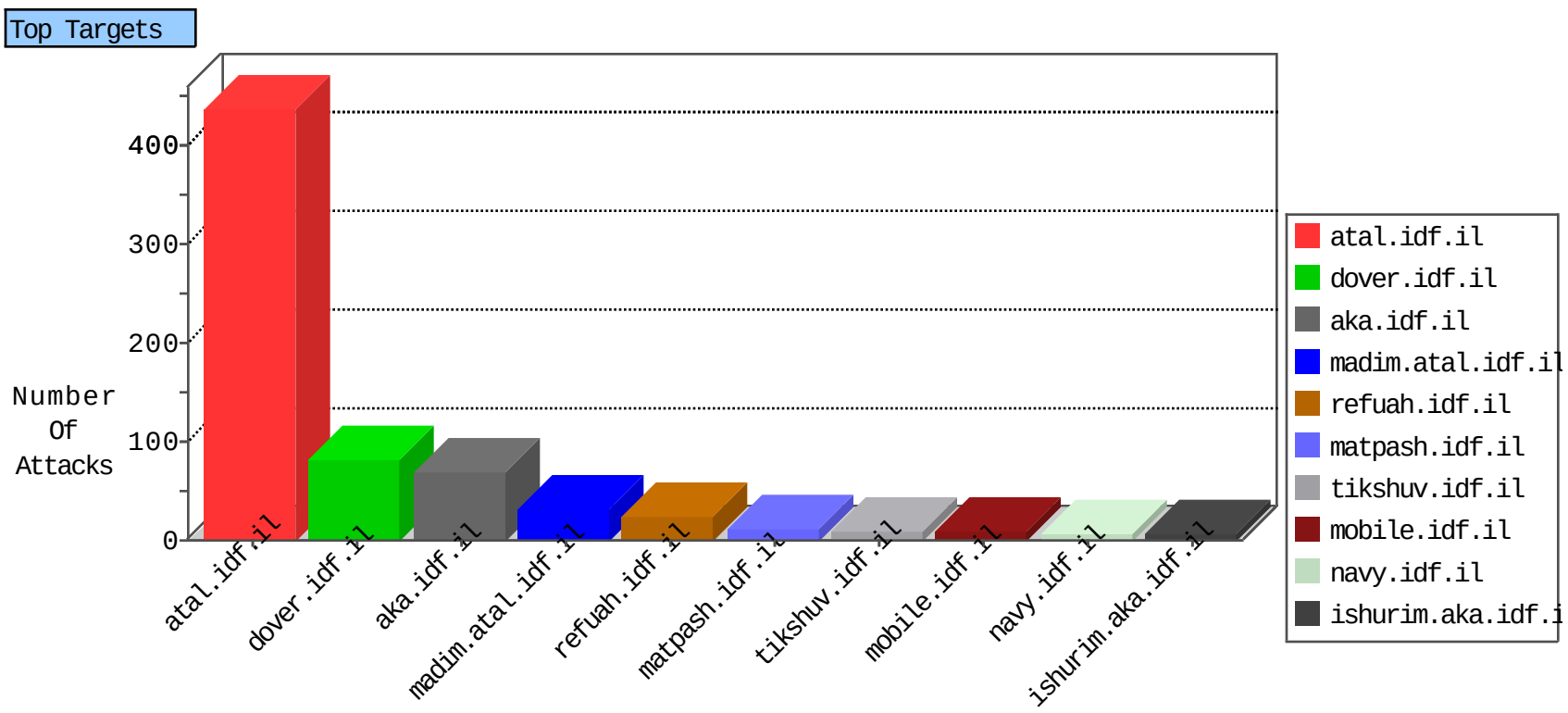
03-27-2015-13:03:04 to 03-27-2015-14:03:04

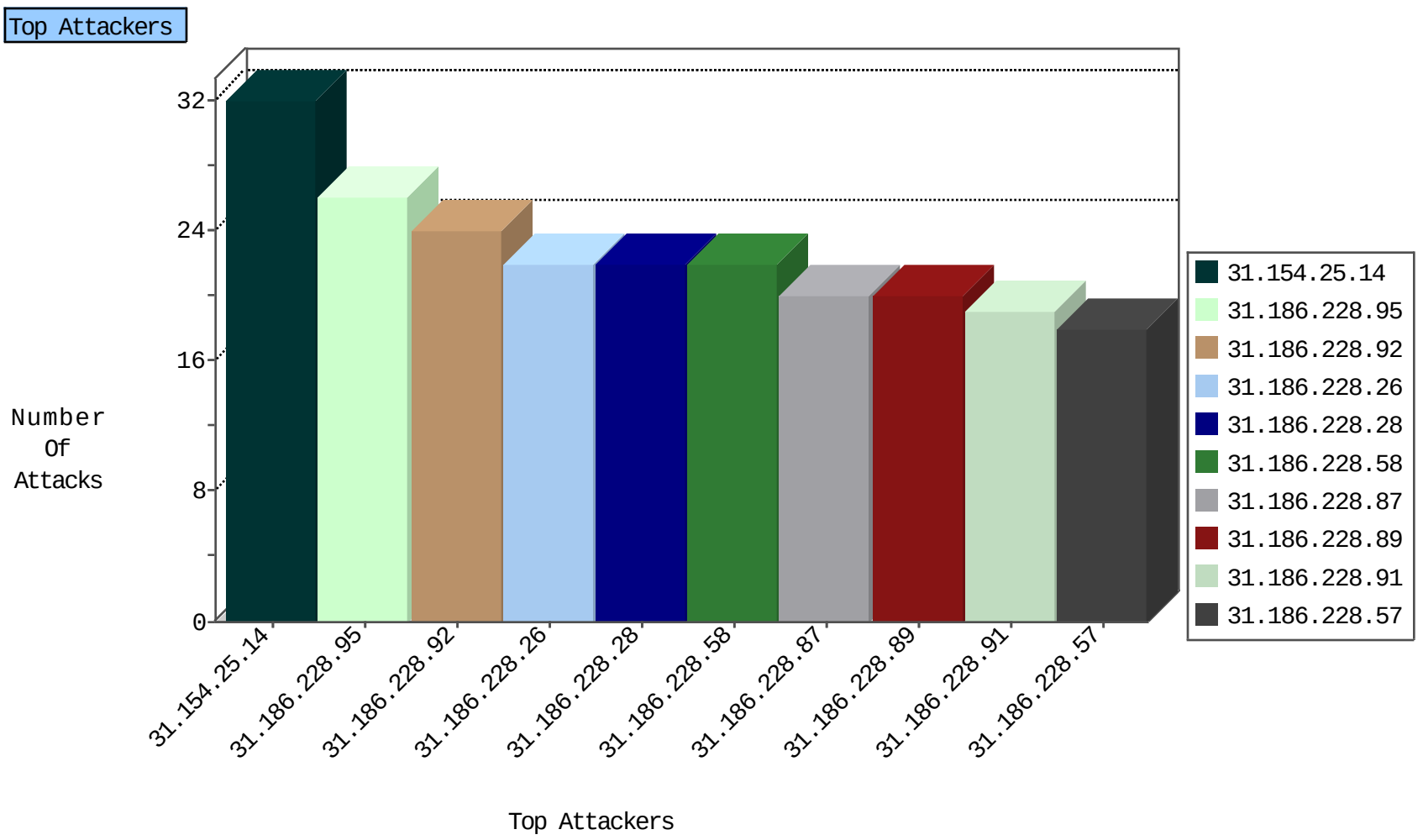
IDF Under Attack
03-27-2015-13:03:04

Top Targets



Top Target

Top Attackers



Top Attackers

03-27-2015-13:03:04 to 03-27-2015-14:03:04

Top Attackers In DDoS-Defence

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

03-27-2015-13:03:04 to 03-27-2015-14:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
212.28.230.202	Lebanon	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
217.243.198.68	Germany	147.237.77.176	matpash.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
46.121.128.156	Israel	147.237.76.31	nakchal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.205.9.131	Slovakia	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
85.250.189.52	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
37.205.9.131	Slovakia	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
109.160.135.175	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.201	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.19.85.226	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

03-27-2015-13:03:04 to 03-27-2015-14:03:04

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	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.67.32	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
37.162.241.23	France	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
104.171.114.254		147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.130	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.160.224.130	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.20.54.249	China	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
128.72.154.6	Russian Federation	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.130	China	147.237.72.217	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.20.54.249	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1

03-27-2015-13:03:04 to 03-27-2015-14:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
31.186.228.95	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	26
31.186.228.92	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	24
31.186.228.26	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	22
31.186.228.28	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	22
31.186.228.58	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	22
31.186.228.87	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	20
31.186.228.89	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	20
31.186.228.91	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	19
31.186.228.57	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	18
31.186.228.94	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.86	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.60	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.96	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.88	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	14
31.186.228.90	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	13
31.186.228.64	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	12
31.186.228.62	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	12
31.186.228.29	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	12
2.54.129.77	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	11
31.186.228.65	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	11
31.186.228.30	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	10
31.186.228.27	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	10
31.186.228.23	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	10
31.186.228.93	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	10
80.253.20.134	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
41.45.163.234	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
46.32.211.13	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	9
31.186.228.31	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	8
31.186.228.170	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	8
80.246.139.25	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
31.186.228.59	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	7
31.186.228.32	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	7
31.186.228.63	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	6
31.186.228.68	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	6
82.102.136.66	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
41.42.170.62	Egypt	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.186.228.61	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	6
31.186.228.24	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	6
31.186.228.67	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	6
31.186.228.25	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	6
31.186.228.66	United Kingdom	147.237.77.233	atal.idf.il	First packet isn't SYN	drop	drop	5
46.19.86.24	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
2.54.11.73	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
109.253.141.158	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
77.114.86.84	Poland	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
188.120.148.211	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
77.114.86.84	Poland	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
2.54.14.189	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	alert	2
2.54.14.189	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	2
93.77.121.43	Ukraine	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
31.154.25.14	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 31.154.25.14	Block	31
79.178.22.200	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 79.178.22.200	Block	7
66.249.67.120	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.67.120	Block	6
66.249.67.128	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.67.128	Block	6
66.249.67.136	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.67.136	Block	4
5.29.19.221	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
207.46.13.5	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 207.46.13.5	Block	3
80.246.139.25	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
89.139.5.208	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.180.5.31	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.180.5.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/main/.com	Block	2
5.29.35.36	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
79.181.126.178	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.181.126.178	Block	2
5.29.218.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.181.126.178	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/6_s3_	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
2.54.155.198	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.241.226.204	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.79.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/idf_in_pictures/2004/february/28.stm	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
94.136.40.78	United Kingdom	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/test/wp-admin/	Block	1
84.108.0.214	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.81.212.190	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/894-he/nakhal.aspx/shared/usercontrols/headerupper/	Block	1
77.125.84.10	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/payslips.aspx	None	1
109.65.192.236	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
93.77.121.43	Ukraine	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
213.251.182.10	France	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wordpress/wp-admin/	Block	1
164.138.124.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/faq/22.stm	Block	1
94.159.171.82	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
31.221.17.219	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
85.64.112.151	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1116-en/dover.aspx	Block	1
79.176.179.99	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
109.253.141.158	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.172.134.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
176.126.201.2	Romania	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-admin/	Block	1
66.249.79.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/information_archive.stm	Block	1
94.180.36.205	Russian Federation	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 94.180.36.205	Block	1
54.172.196.207	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
85.65.226.220	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 85.65.226.220	Block	1
207.46.13.5	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/news/news.aspx	Block	1
149.88.3.88	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.172.134.246	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
185.32.179.26	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.142.232.6	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/blog/wp-admin/	Block	1
94.180.36.205	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/homepage.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
54.211.236.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2000/october/8.stm	Block	1
85.65.226.220	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/links/6_s3_	Block	1
79.178.22.200	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/idf_in_pictures/2000/october/piguim.stm	Block	1