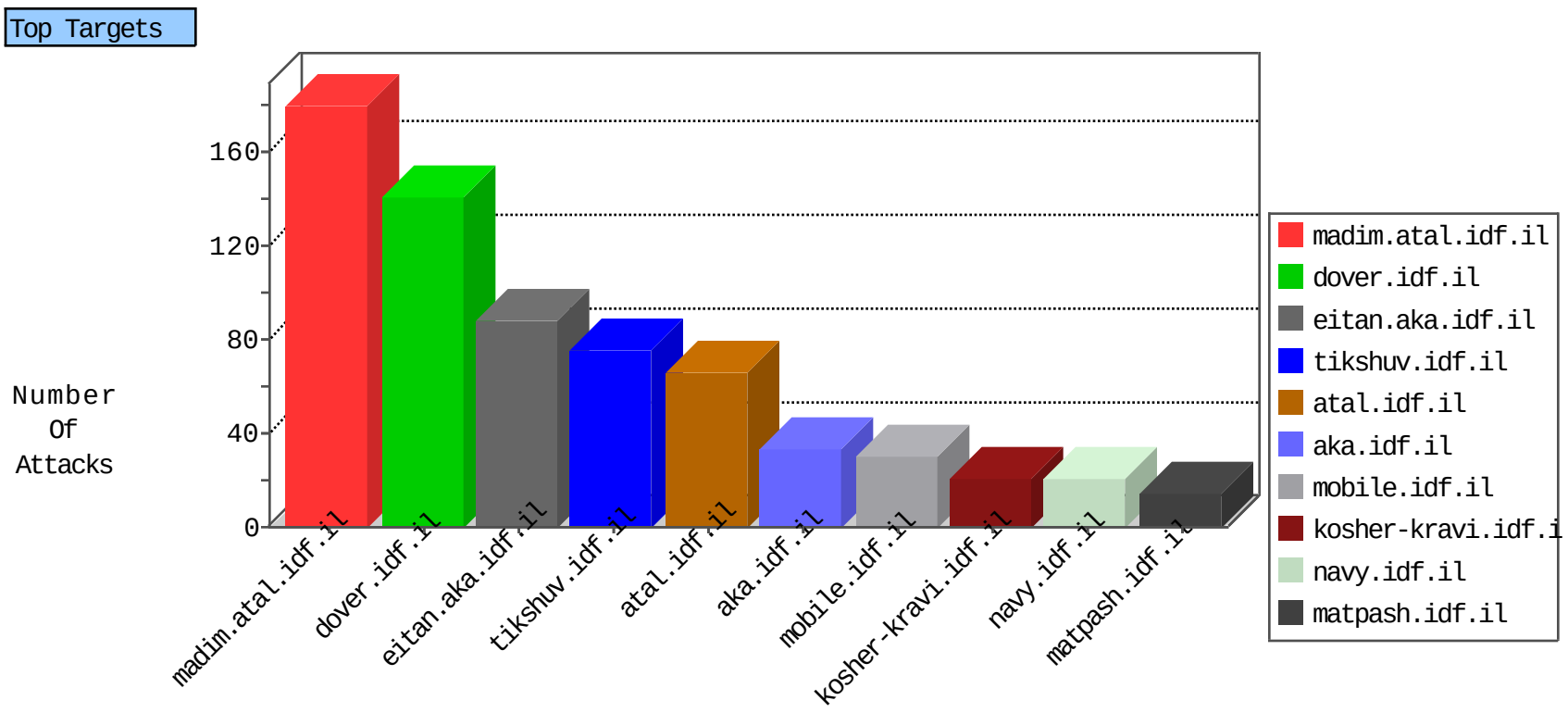
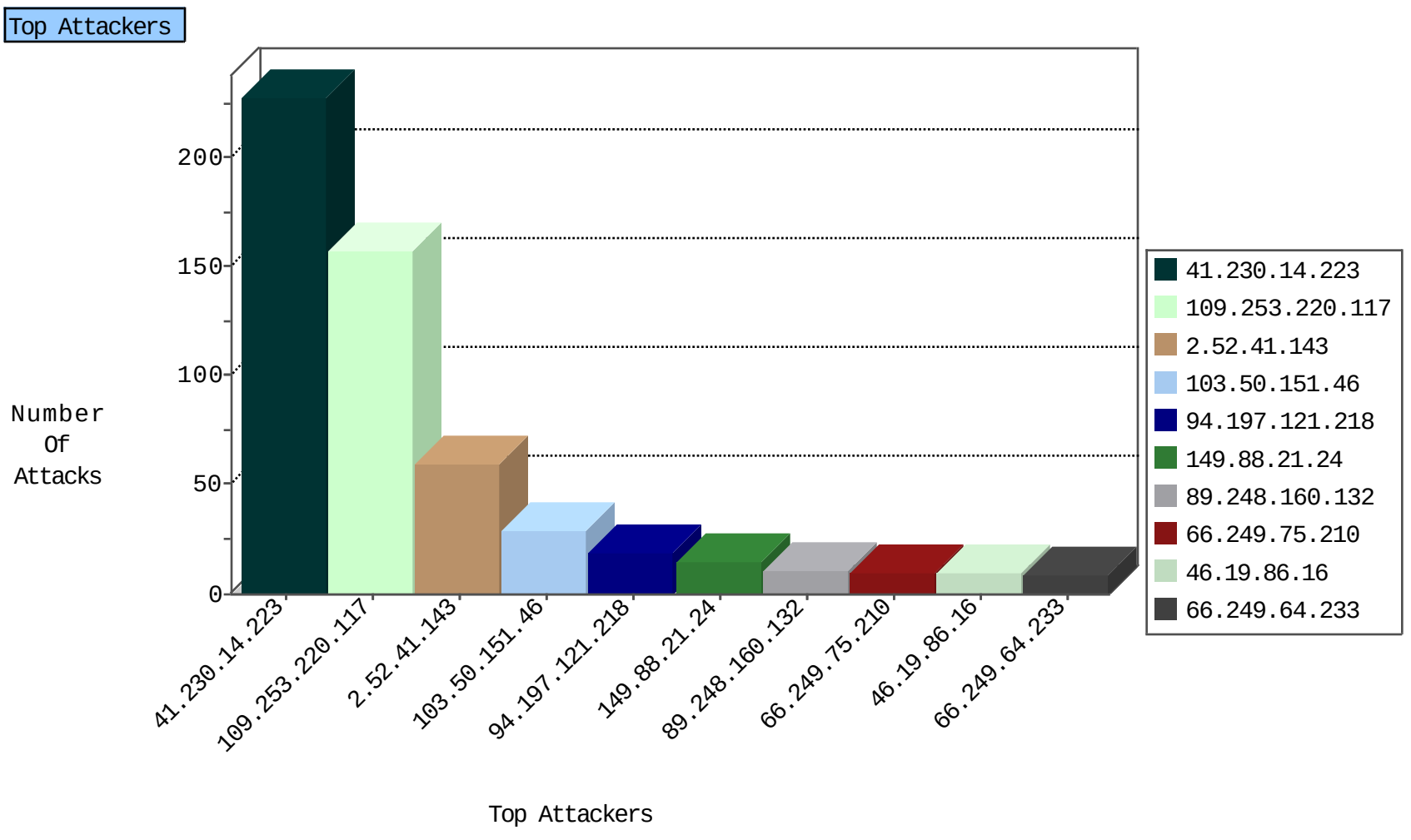
03-06-2016-06:04:07 to 03-06-2016-07:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-06-2016-06:04:07 to 03-06-2016-07:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
184.105.247.252	United States	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.84	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.112	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
207.141.11.146	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.88	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.120	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.76	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
219.161.116.188	Japan	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.100	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.84	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
66.240.236.119	United States	147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.108	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.72	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1

03-06-2016-06:04:07 to 03-06-2016-07:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.41.63	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
195.154.252.118	France	147.237.76.200	eitan.aka.idf.il	22611: HTTP: WordPress LoginWall Fake Plugin Usage	Block	1

03-06-2016-06:04:07 to 03-06-2016-07:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
209.126.116.147	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
113.59.33.61	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
63.221.141.195	147.237.0.15	Hong Kong	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
63.221.141.195	147.237.0.17	Hong Kong	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

03-06-2016-06:04:07 to 03-06-2016-07:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	78
41.230.14.223	Tunisia	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	70
41.230.14.223	Tunisia	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	49
41.230.14.223	Tunisia	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
149.88.21.24	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.52.41.143	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
66.249.75.210	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
103.50.151.46		147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	10
46.19.86.16	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.52.41.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
103.50.151.46		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.75.218	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.41.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.52.41.143	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.52.41.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
2.52.41.143	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	5
103.50.151.46		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
103.50.151.46		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.197.121.218	United Kingdom	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
177.230.217.184	Mexico	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
103.50.151.46		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
94.197.121.218	United Kingdom	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
94.197.121.218	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
37.26.146.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.145.82	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.69.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.197.121.218	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.182.103.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.138.14	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.22.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
83.166.234.6	Russian Federation	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
46.19.86.87	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.60.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.197.121.218	United Kingdom	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
2.52.41.143	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
195.10.197.89	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
195.10.197.89	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
37.26.147.222	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.52.41.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
2.52.41.143	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
2.54.181.99	Israel	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
94.197.121.218	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
37.26.147.222	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.130.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.75.226	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
54.167.183.116	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.52.41.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.220.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	157
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	9
2.52.41.143	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	9
79.177.145.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.41.143	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.178.218.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.138.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	2
79.177.145.82	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	2
66.249.64.61	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2254.jpg	Block	1
203.133.171.34	Korea, Republic of	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
31.168.101.163	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Unknown Parameter tab in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
213.8.204.24	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
193.225.36.84	Hungary	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf_in_pictures/hasata/thumb.jpg	Block	1
94.23.38.15	France	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp/wp-admin/	Block	1
37.26.146.229	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.70	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
124.193.211.11	China	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
41.230.14.223	Tunisia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	1
213.8.204.24	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 213.8.204.24	Block	1
195.154.252.118	France	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	1
94.26.140.150	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized Request Content Type text/html	Block	1
37.247.54.2	Italy	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/old/wp-admin/	Block	1
207.241.237.223	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/iturim/asp/displayonesoldier.asp	None	1
149.88.201.236	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
213.8.204.24	Israel	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
41.230.14.223	Tunisia	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	1
195.154.252.118	France	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/wp-content/plugins/archive.php	Block	1
94.26.140.150	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sys-admin-message_google_is_not_our_friend_and_the_monoply_rip-off_needs_to_be_stopped	Block	1
66.249.66.23	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1065-en/dover.aspx	Block	1
184.105.247.195	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
83.166.234.6	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
213.8.204.24	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
66.249.64.51	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
199.30.25.142	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
24.138.71.52	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.73.227	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/8/4538.pdf	Block	1
41.230.14.223	Tunisia	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SortDir in www.eitan.aka.idf.il/1103-en/eitan.aspx	None	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1384-he/dover.aspx	Block	1
192.115.248.2	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
85.233.160.38	United Kingdom	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/blog/wp-admin/	Block	1

03-06-2016-06:04:07 to 03-06-2016-07:04:07