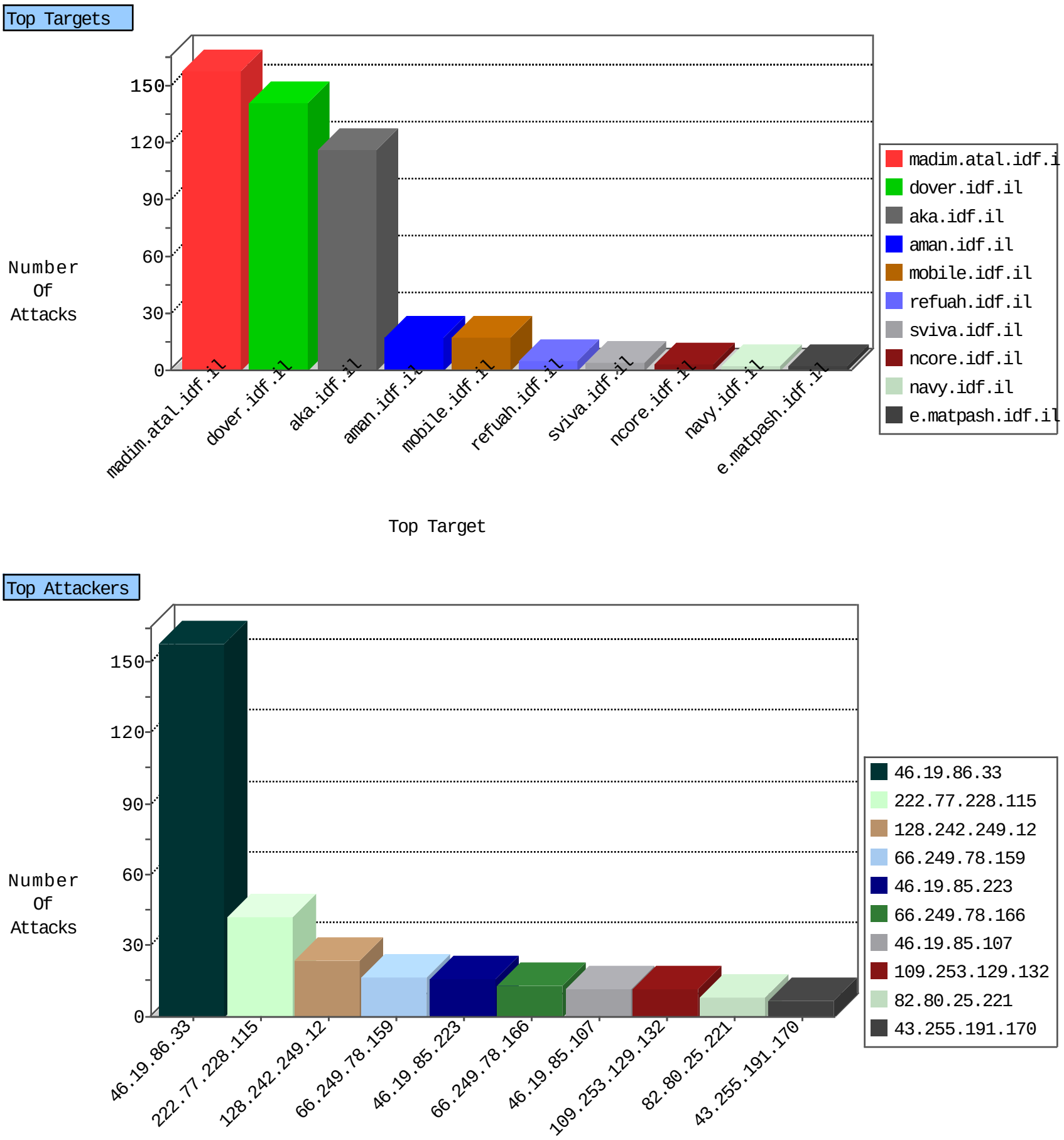
03-29-2015-06:03:00 to 03-29-2015-07:03:00

IDF Under Attack
03-29-2015-06:03:00



03-29-2015-06:03:00 to 03-29-2015-07:03:00

Top Attackers In DDoS-Defence

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

03-29-2015-06:03:00 to 03-29-2015-07:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
222.77.228.115	China	147.237.72.166	aka.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	34
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	24
85.25.43.94	Germany	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1

03-29-2015-06:03:00 to 03-29-2015-07:03:00

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
61.240.144.64	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
190.122.98.91	Dominican Republic	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.170	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
190.122.98.91	Dominican Republic	147.237.77.235	sviva.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.170	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
121.37.40.100	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
61.158.162.40	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.170	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
193.107.16.206	Russian Federation	147.237.77.19	law-forum.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
43.255.191.170	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
190.122.98.91	Dominican Republic	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.170	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
121.37.40.100	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
121.37.40.100	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.67	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1

03-29-2015-06:03:00 to 03-29-2015-07:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.85.223	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	16
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
109.253.129.132	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
46.19.85.107	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	12
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
66.249.75.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.75.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
109.253.136.236	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
176.12.140.132	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
222.77.228.115	China	147.237.72.166	aka.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	4
176.12.141.63	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
176.12.141.213	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
109.253.131.12	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
176.12.137.194	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
176.12.146.7	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
80.246.136.62	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
176.12.141.27	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
5.102.254.191	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
2.54.34.41	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	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
66.249.75.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
2.54.34.41	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
66.249.81.206	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
2.54.34.41	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
66.249.67.58	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
176.12.136.165	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
66.249.81.212	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
188.165.15.148	France	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
176.12.136.165	Israel	147.237.77.243	mobile.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
66.249.81.230	United States	147.237.77.176	matpash.idf.il	directory traversal overflow	Directory Traversal	monitor	1
74.82.47.31	United States	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.86.251	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
216.218.206.83	United States	147.237.76.148	gqcenter.aka.idf.i		drop	drop	1
66.249.78.153	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
184.105.139.67	United States	147.237.76.42	refuah.idf.il	SAM rule	drop	drop	1
124.202.190.60	China	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
66.249.81.209	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
216.218.206.112	United States	147.237.76.200	eitan.aka.idf.il		drop	drop	1
81.218.15.198	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
184.105.139.84	United States	147.237.77.61	e.cogat.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.19.86.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	144
185.32.176.119	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
157.55.39.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.42	Block	3
198.204.249.34	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.aspx	Block	3
109.253.156.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.6	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	2
222.77.228.115	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
93.172.168.195	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 93.172.168.195	Block	2
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//994-8613-he/navy.aspx.aspx	Block	2
176.12.137.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.131.12	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.81.230	United States	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/../favicon.ico	Block	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.16	Block	1
176.12.148.2	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.168.90.249	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl18.y in www.aka.idf.il/main/sachar/viewpniot.aspx	None	1
134.0.10.218	Spain	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
216.98.149.238	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
84.110.109.125	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$txtKerenHistalmoot in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/search.asp	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	1
176.12.140.163	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.132.164	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/2004/january/0120-2.stm	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/chaplaincy/chaplain.stm	Block	1
176.12.150.96	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.168.90.249	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl26.y in www.aka.idf.il/main/sachar/viewpniot.aspx	None	1
222.77.228.115	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 222.77.228.115	Block	1
87.69.235.153	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/default.aspx	None	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/faq/7.stm	Block	1
176.12.141.27	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.52.177.30	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.253.135.185	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.79	United States	147.237.72.166	aka.idf.il	Unknown Parameter pageNum in www.aka.idf.il/chinuch/faq/default.asp	None	1
70.167.8.42	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/564-en/sb_item_lev1_s	Block	1
180.76.4.87	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
176.12.141.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.168.90.249	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
185.4.73.68	Estonia	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.78.104	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
176.12.136.29	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.172.168.195	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	1
222.77.228.115	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ckeditor/ckfinder/core/connector/asp/connector.asp	Block	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//atal1/izkor/search.asp	Block	1
199.203.171.197	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
176.12.146.7	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.168.90.249	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/viewpniot.aspx	None	1
124.202.190.60	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1

03-29-2015-06:03:00 to 03-29-2015-07:03:00