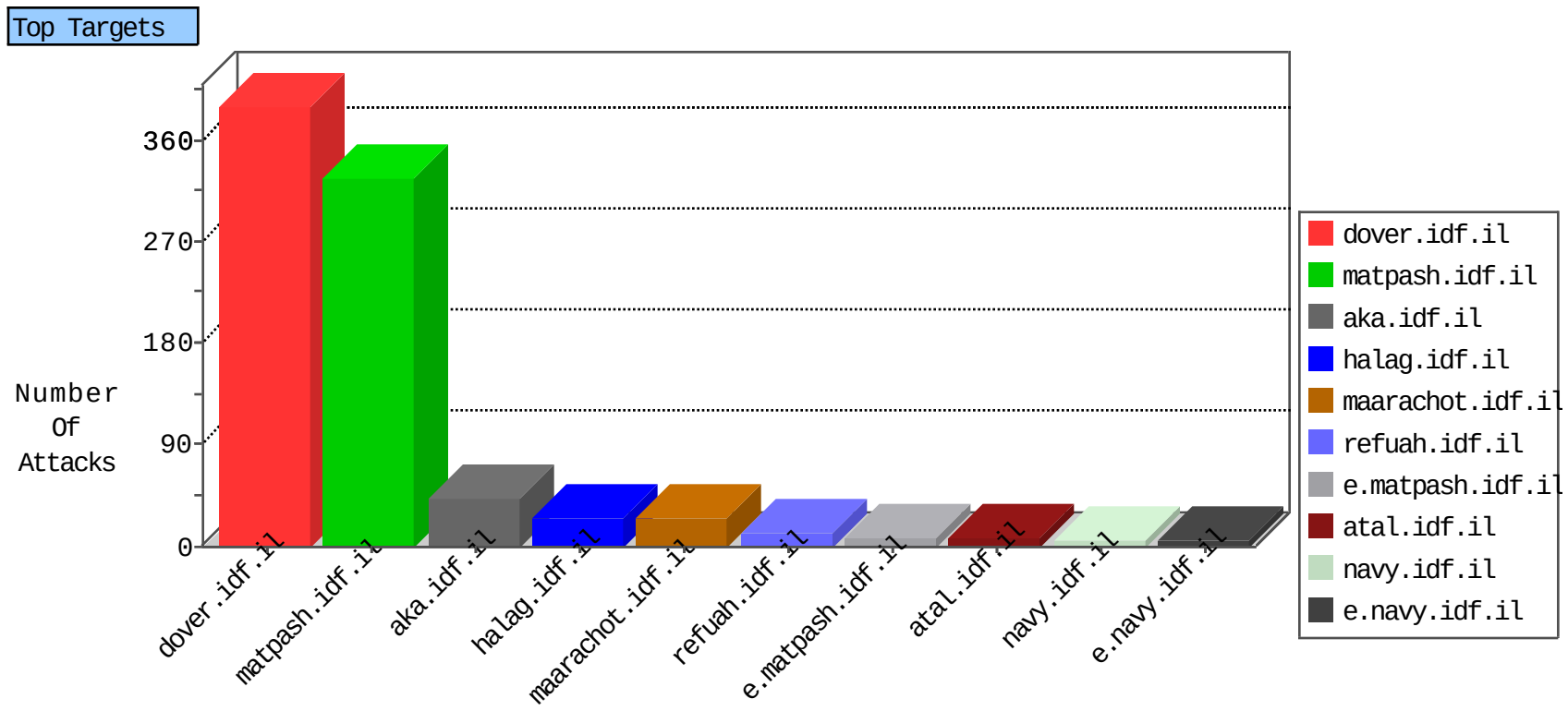
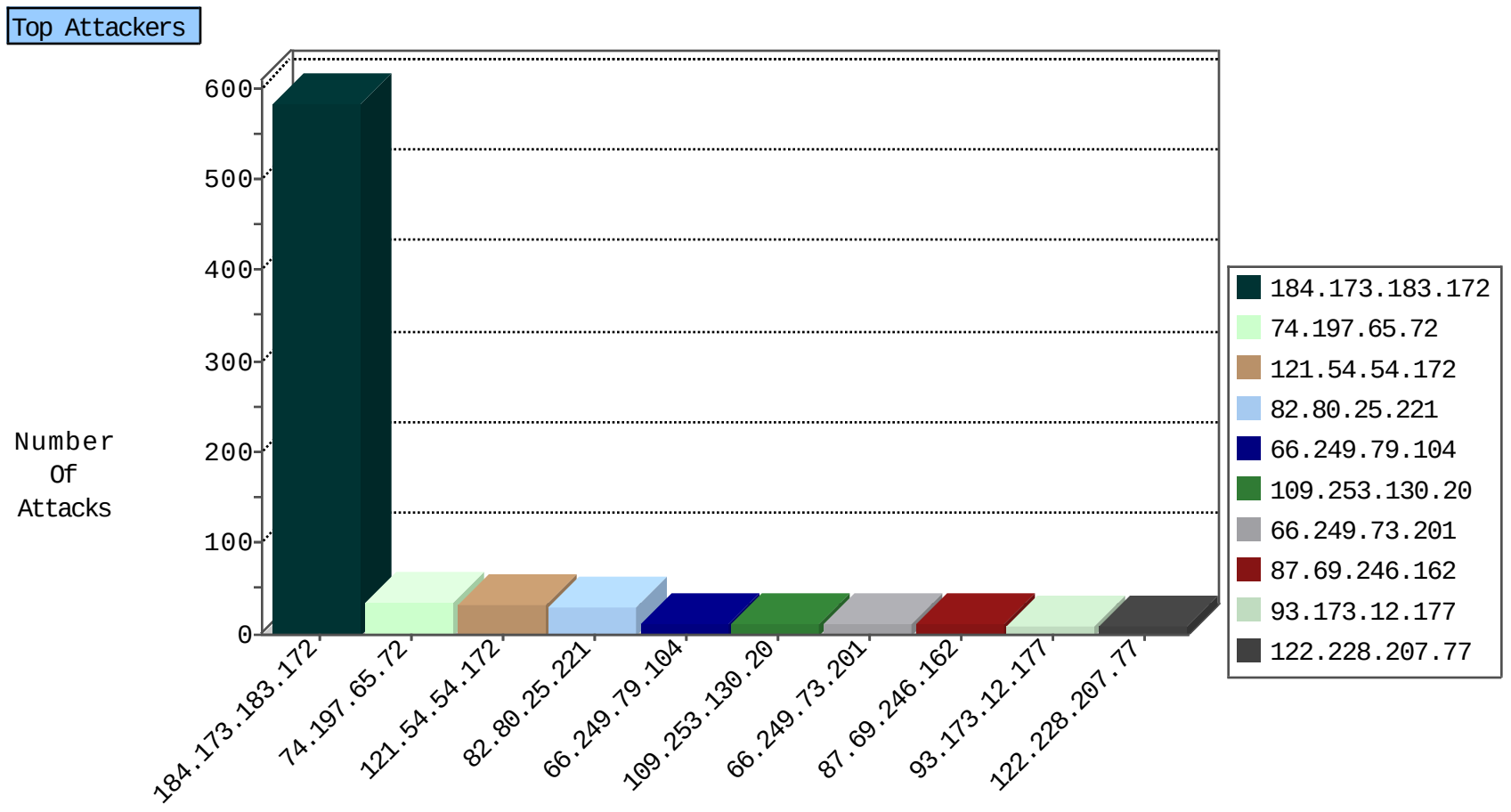
03-28-2015-10:03:04 to 03-28-2015-11:03:04

IDF Under Attack
03-28-2015-10:03:04

Top Targets



Top Attackers



03-28-2015-10:03:04 to 03-28-2015-11:03:04

Top Attackers In DDoS-Defence

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

03-28-2015-10:03:04 to 03-28-2015-11:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.176	matpash.idf.il	DVRep_P-N_40-59	Permit	319
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	265
93.173.38.66	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
46.19.85.154	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
37.130.227.133	United Kingdom	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1

03-28-2015-10:03:04 to 03-28-2015-11:03:04

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	29
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.75.68	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
109.65.181.100	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
122.228.207.77	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
202.142.147.190	Pakistan	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 4096	1
95.0.126.16	Turkey	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
202.142.147.190	Pakistan	147.237.76.86	navy.idf.il	ET SCAN NMAP -f -sS	1
95.0.126.16	Turkey	147.237.76.42	refuah.idf.il	ET SCAN NMAP -f -sS	1
196.47.173.21	Cote D'Ivoire	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
74.197.65.72	United States	147.237.77.176	matpash.idf.il	SERVER-WEBAPP bad HTTP/1.1 request, Potentially worm attack	1
196.47.173.21	Cote D'Ivoire	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
122.228.207.77	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.77	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
61.158.162.40	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.77	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
202.142.147.190	Pakistan	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 2048	1
95.0.126.16	Turkey	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
199.59.148.211	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	Cote D'Ivoire	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
74.197.65.72	United States	147.237.77.170	maarachot.idf.il	SERVER-WEBAPP bad HTTP/1.1 request, Potentially worm attack	1
61.240.144.67	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

03-28-2015-10:03:04 to 03-28-2015-11:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
121.54.54.172	Philippines	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	33
66.249.73.201	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.79.104	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.253.130.20	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.79.96	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
93.173.12.177	Israel	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	8
87.69.246.162	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
109.253.136.59	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
74.197.65.72	United States	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
2.92.176.142	Russian Federation	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
74.197.65.72	United States	147.237.77.121	e.navy.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
87.69.246.162	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	alert	4
74.197.65.72	United States	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
74.197.65.72	United States	147.237.77.227	e.hamaz.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
66.249.79.112	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
74.197.65.72	United States	147.237.77.205	prisha.idf.il	SAM rule	drop	drop	2
74.197.65.72	United States	147.237.77.233	atal.idf.il	SAM rule	drop	drop	2
188.120.148.136	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
74.197.65.72	United States	147.237.77.234	halag.idf.il	SAM rule	drop	drop	2
74.197.65.72	United States	147.237.77.216	dover.idf.il	SAM rule	drop	drop	2
74.197.65.72	United States	147.237.77.235	sviva.idf.il	SAM rule	drop	drop	2
74.197.65.72	United States	147.237.77.226	www.chamatz.aka.idf.il	SAM rule	drop	drop	2
74.197.65.72	United States	147.237.77.243	mobile.idf.il	SAM rule	drop	drop	2
46.19.85.185	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
2.52.39.54	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
85.64.151.71	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
192.3.24.223	United States	147.237.77.216	dover.idf.il	header rejection pattern found in request	Header Rejection	monitor	1
62.0.228.129	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
141.212.122.176	United States	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
38.99.240.151	United States	147.237.76.42	refuah.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
89.138.70.158	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
70.39.187.108	Satellite Provide	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
46.19.85.186	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
118.96.230.10	Indonesia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
2.54.38.187	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
87.69.194.94	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
141.212.122.182	United States	147.237.8.14	e.orchot.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
41.82.43.232	Senegal	147.237.77.233	atal.idf.il	header rejection pattern found in request	Header Rejection	monitor	1
89.138.70.158	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
74.82.47.46	United States	147.237.0.35	akaws.idf.il		drop	drop	1
188.120.148.136	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.75	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
87.69.194.94	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
216.218.206.107	United States	147.237.77.121	e.navy.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.195	United States	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.85.53	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
188.138.17.205	France	147.237.76.147	chinuch.aka.idf.il		drop	drop	1
46.120.137.220	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.85	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
109.186.51.32	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
213.251.182.10	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
79.180.163.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	3
5.29.137.220	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 5.29.137.220	Block	3
87.69.81.112	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
74.197.65.72	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 74.197.65.72	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
192.3.24.223	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
66.249.69.42	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.69.42	Block	1
74.197.65.72	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 74.197.65.72	Block	1
66.249.75.60	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
176.12.143.237	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.29.137.220	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
84.228.60.59	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/tfasim.aspx	None	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.42	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/×©×§×• ×¤×™×ª×ª 9	Block	1
207.46.13.104	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1098-7637-he/atal.aspx	Block	1
109.253.130.250	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
74.197.65.72	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
66.249.75.117	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.75.117	Block	1
188.165.15.60	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-5857-he/patzar.aspx	Block	1
41.82.43.232	Senegal	147.237.77.233	atal.idf.il	E-mail collector robots 14	Block	1
70.167.8.42	United States	147.237.72.166	aka.idf.il	Abnormally Long Request request version	Block	1
66.249.73.193	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1125-1.stm	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	Block	1
109.253.134.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.117	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/brothers	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0115-1.stm	Block	1
41.82.43.232	Senegal	147.237.77.233	atal.idf.il	eMail Hoarding	Block	1
87.69.178.68	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
70.167.8.42	United States	147.237.72.166	aka.idf.il	Illegal HTTP Version ???????? ???????????? ???? ?????????? ???????? ?? HTTP/1.1	Block	1
66.249.75.13	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.75.13	Block	1
207.46.13.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/arabic1.stm	Block	1
109.253.149.140	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.187.127	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.79.49	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
192.3.24.223	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
46.116.219.242	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/faqselection.aspx	None	1
93.173.12.177	Israel	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
66.249.75.13	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch	Block	1
212.29.220.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
125.209.235.184	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
79.182.126.208	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in aka.idf.il/main/sachar/payslips.aspx	None	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/123103-3.stm	Block	1