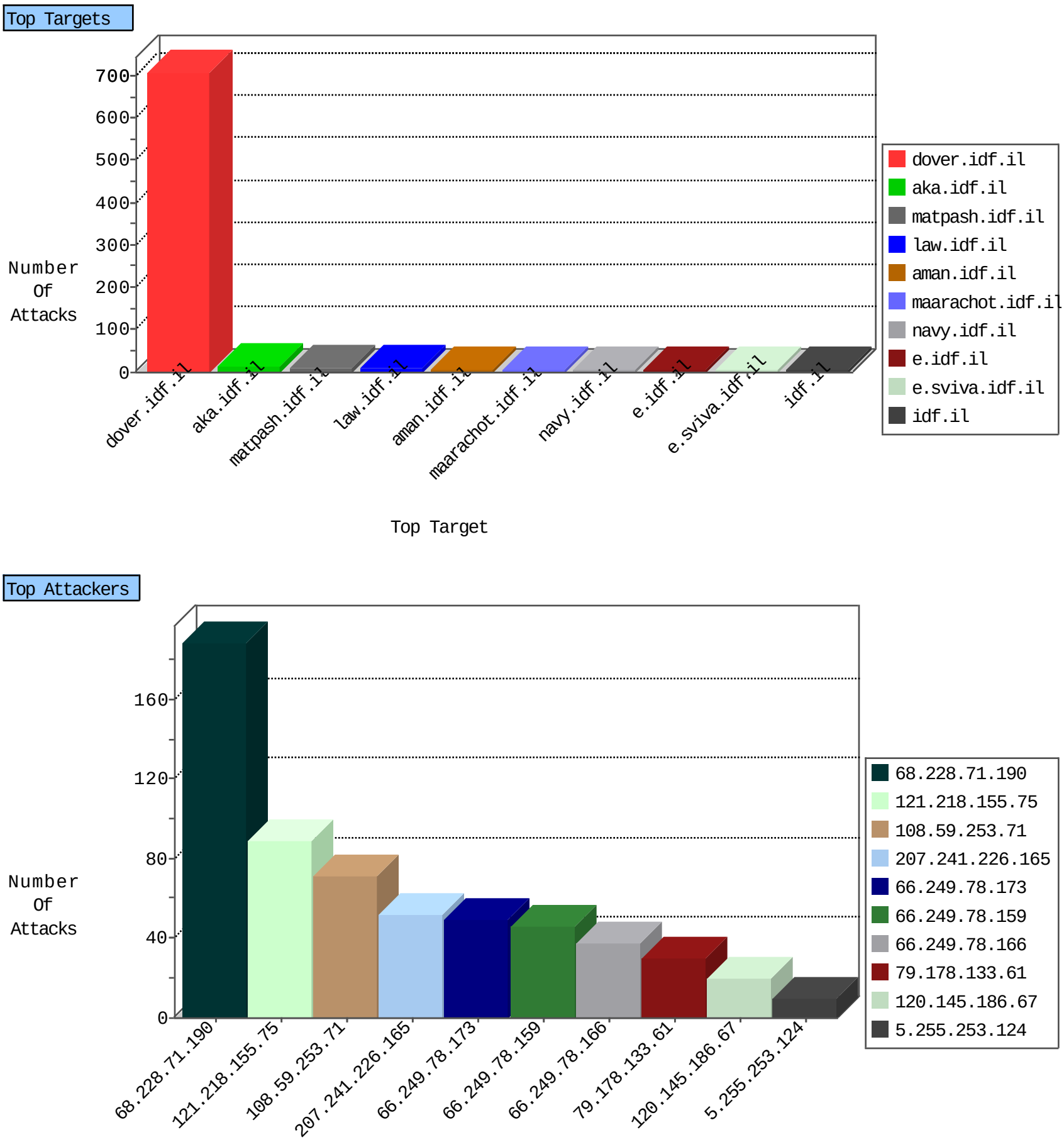
04-18-2015-04:03:07 to 04-18-2015-05:03:07

IDF Under Attack
04-18-2015-04:03:07



04-18-2015-04:03:07 to 04-18-2015-05:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.40	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	268
84.228.58.171	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	3
218.209.187.243	Korea, Republic of	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2
124.232.142.220	China	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
124.232.142.220	China	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

04-18-2015-04:03:07 to 04-18-2015-05:03:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
198.20.70.114	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
96.44.189.101	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1

04-18-2015-04:03:07 to 04-18-2015-05:03:07

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
66.249.65.28	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.24	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
218.6.132.45	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 4096	1
218.6.132.45	China	147.237.0.33	idf.il	ET SCAN NMAP -f -sS	1
210.252.145.146	Japan	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
202.71.25.29	India	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
37.220.34.55	Netherlands	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
218.6.132.45	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 2048	1
210.252.145.146	Japan	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
210.252.145.146	Japan	147.237.0.35	akaws.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.67	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
37.220.34.55	Netherlands	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1

04-18-2015-04:03:07 to 04-18-2015-05:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
68.228.71.190	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	189
121.218.155.75	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	89
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	71
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	42
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	40
207.241.226.165	United States	147.237.77.216	dover.idf.il	Web Servers Slow HTTP Denial of Service	Web Server Enforcement Violation	reject	38
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
79.178.133.61	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
120.145.186.67	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
207.241.226.165	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
148.251.41.235	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.210.202.185	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
24.239.71.237	United States	147.237.72.217	e.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
70.209.48.106	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
200.225.203.77	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
189.166.173.182	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.210.202.185	Israel	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	3
204.237.22.235	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
79.178.182.149	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.64.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
128.242.249.10	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
79.182.57.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
84.111.155.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
107.170.181.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.6	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
136.243.36.88	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.160.221.93	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.116.171.75	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
89.139.40.161	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
95.173.189.7	Turkey	147.237.77.212	e.dover.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
173.252.110.113	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
198.48.92.104	United States	147.237.76.196	e.sviva.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
173.252.110.119	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
198.48.92.104	United States	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
66.249.64.76	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
184.105.247.211	United States	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.85.232	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
198.48.92.104	United States	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
157.55.39.33	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	7
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	4
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	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
92.43.16.46	Spain	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
66.249.65.186	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
157.55.39.33	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19021-he/dover.aspx×³Ö³Â¯Ö²Â¿Ö²Â½×³Â?×³Ö³Â¯Ö²Â¿Ö²Â½×³Ö³Â¯Ö²Â¿Ö²Â½×³Â£	Block	1
106.51.135.164	India	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
188.143.232.72	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
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter cat... in www.aka.idf.il/kamlar/klali/default.asp	None	1
148.251.41.235	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/grapheat.stm	Block	1
74.82.47.2	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1
157.55.39.130	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/faq/	Block	1
46.19.85.169	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
107.153.7.122	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0215-1.stm	Block	1
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catID in www.aka.idf.il/kamlar/home/default.asp	None	1
203.133.168.157	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.4	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
92.43.16.46	Spain	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17802-he/dover.aspx	Block	1
162.255.166.53		147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
46.120.120.121	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
120.15.43.54	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 120.15.43.54	Block	1
66.249.64.63	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.63	Block	1
203.133.168.157	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18762-he/dover.aspx	Block	1
185.10.104.132	Europe	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/901-9403-he/cogat.aspx	Block	1
49.48.127.186	Thailand	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/14-en/patzar.aspx	Block	1
120.15.43.54	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/getfile/getfile.aspx/trackback/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	1
66.249.65.28	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
207.46.13.22	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.158.145.28	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
187.74.123.146	Brazil	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.64.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
148.251.41.235	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 148.251.41.235	Block	1