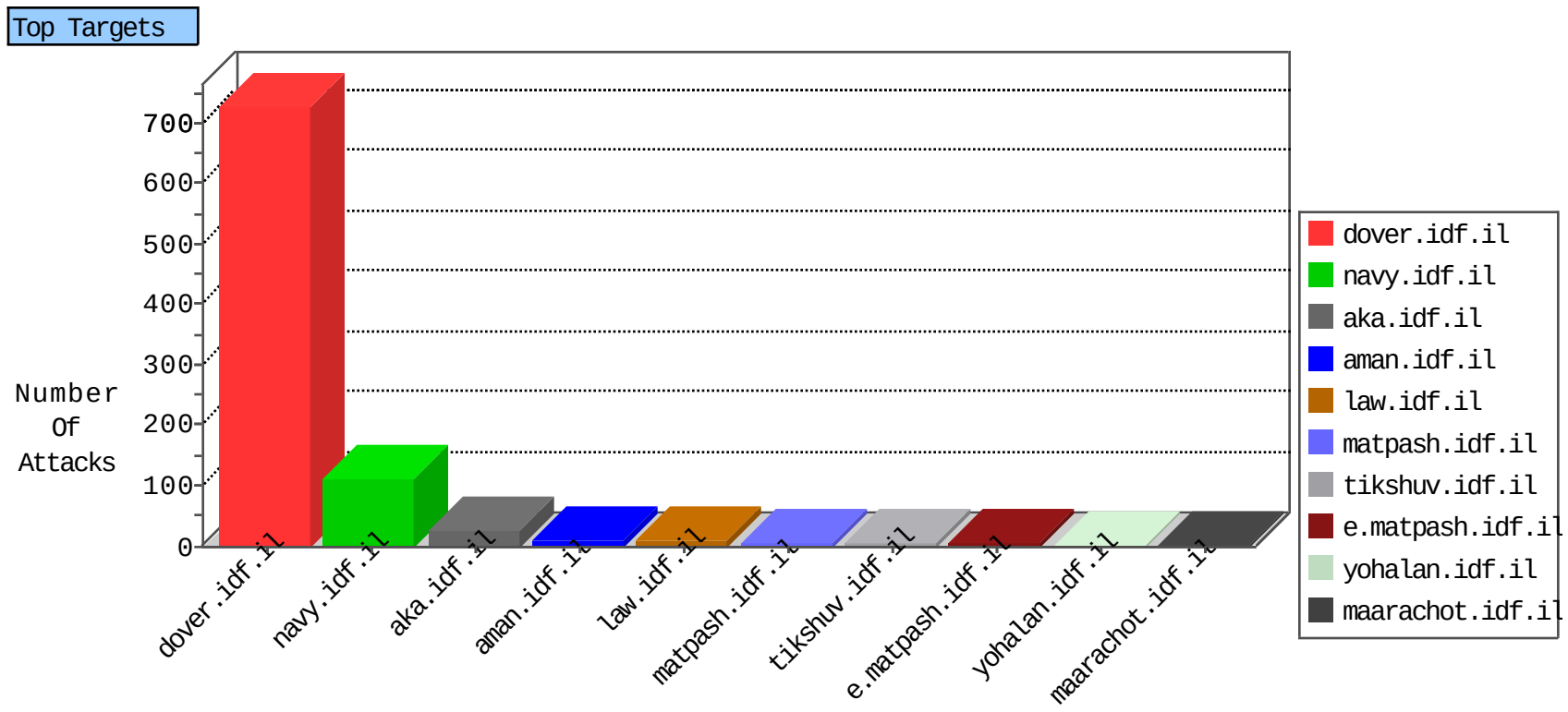
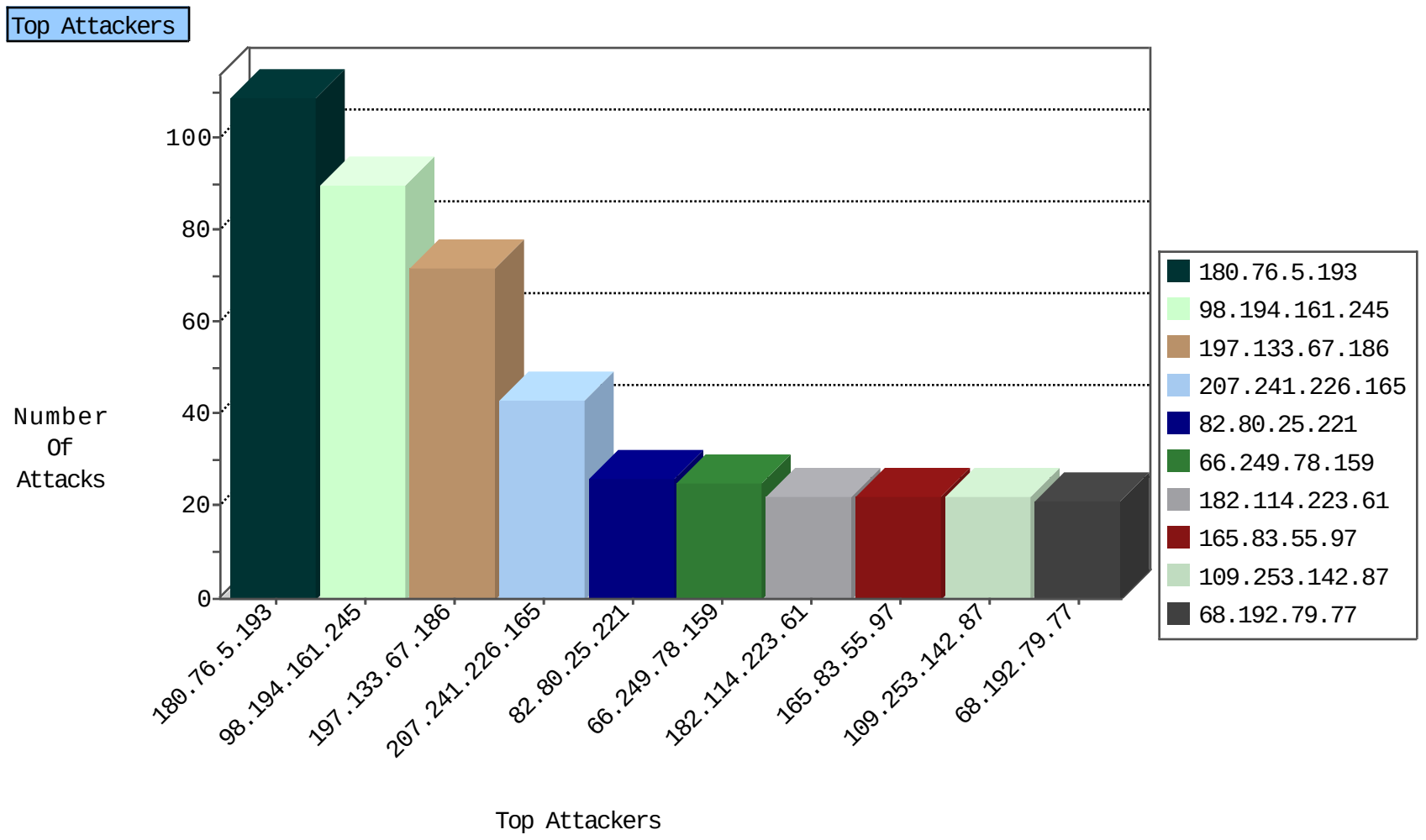
04-18-2015-05:03:08 to 04-18-2015-06:03:08

IDF Under Attack
04-18-2015-05:03:08

Top Targets



Top Attackers



04-18-2015-05:03:08 to 04-18-2015-06:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
219.160.73.197	Japan	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1

04-18-2015-05:03:08 to 04-18-2015-06:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	109
182.114.223.61	China	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	12
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
85.25.103.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	2
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.86	navy.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	147.237.77.178	e.matpash.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1

04-18-2015-05:03:08 to 04-18-2015-06:03:08

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	26
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
60.208.72.139	China	147.237.77.216	dover.idf.il	GPL SCAN nmap TCP	4
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	4
66.249.67.40	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
66.249.73.219	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.166	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.65	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
111.13.30.109	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 4096	1
101.226.2.99	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
73.222.216.129	United States	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
73.222.216.129	United States	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
193.189.246.45	Germany	147.237.0.34	tikshuv.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
61.240.144.64	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
111.13.30.109	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
101.226.2.99	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -f -sS	1
73.222.216.129	United States	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
73.222.216.129	United States	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
73.222.216.129	United States	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1

04-18-2015-05:03:08 to 04-18-2015-06:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
98.194.161.245	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	90
197.133.67.186	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	72
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	25
165.83.55.97	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
109.253.142.87	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
68.192.79.77	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
192.151.151.202	United States	147.237.77.216	dover.idf.il	SAM rule	drop	drop	19
109.253.145.24	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
207.241.226.165	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
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
68.195.41.118	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	10
136.243.36.88	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
129.10.9.17	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
192.116.162.182	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
72.234.197.144	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
182.114.223.61	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
207.46.13.77	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
2.54.19.230	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
171.98.76.157	Thailand	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
189.18.165.56	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
222.84.2.167	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
85.72.40.4	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
65.26.20.236	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
2.54.33.149	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
204.237.22.235	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.247.36.78	Netherlands	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
5.29.28.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
60.208.102.75	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
166.182.3.58	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
166.182.3.239	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
166.182.3.133	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
207.46.13.35	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
95.187.205.136	Romania	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
189.251.255.22	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
166.182.3.28	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.51	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
166.182.3.167	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

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	6
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	4
54.209.60.63	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
66.249.73.166	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/m/	Block	1
207.46.13.35	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-18630-he/dover.aspx×³Ö³Æ’Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â½×³Â©×³Ö³Æ’Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â½"×³Ö³Æ’Ö¶â€™Ö³â€šÖ²Â¯Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ’×’â,¬ÂšÖ³â€šÖ²Â½,	Block	1
176.10.104.234	Switzerland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-en/	Block	1
69.12.81.9	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/grapheat.stm	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
184.105.247.195	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.64.72	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0306-4.stm	Block	1
95.173.184.138	Turkey	147.237.76.30	himush.idf.il	Illegal HTTP Version	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
207.46.13.77	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.77	Block	1
180.76.4.148	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
69.12.82.145	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
188.165.15.206	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.84	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
95.173.189.7	Turkey	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/6/1446.pdf/	Block	1
207.46.13.77	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/doc/	Block	1
180.76.6.46	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/901-7721-he/tikshuv.aspx	Block	1
58.22.77.143	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp/trackback/	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20063-he/idfgdover.aspx	Block	1
66.249.64.86	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
203.151.27.79	Thailand	147.237.77.74	law.idf.il	Illegal HTTP Version	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
207.46.13.104	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
182.114.223.61	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 182.114.223.61	Block	1
66.249.64.58	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/m/	Block	1
74.82.47.2	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.78.127	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/mobile/	Block	1
66.249.64.88	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//main/giyus/giyus/general.aspx	Block	1
207.46.13.35	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.35	Block	1
176.10.104.234	Switzerland	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 176.10.104.234	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/unitfs.asp	Block	1
207.46.13.104	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.73.213	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
182.114.223.61	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/editor/editor/filemanager/connectors/aspx/connector.aspx	Block	1
66.249.64.70	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
84.108.121.180	Israel	147.237.72.166	aka.idf.il	Unknown Parameter isTaz in www.aka.idf.il/main/sachar/	None	1
66.249.78.134	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/m/	Block	1