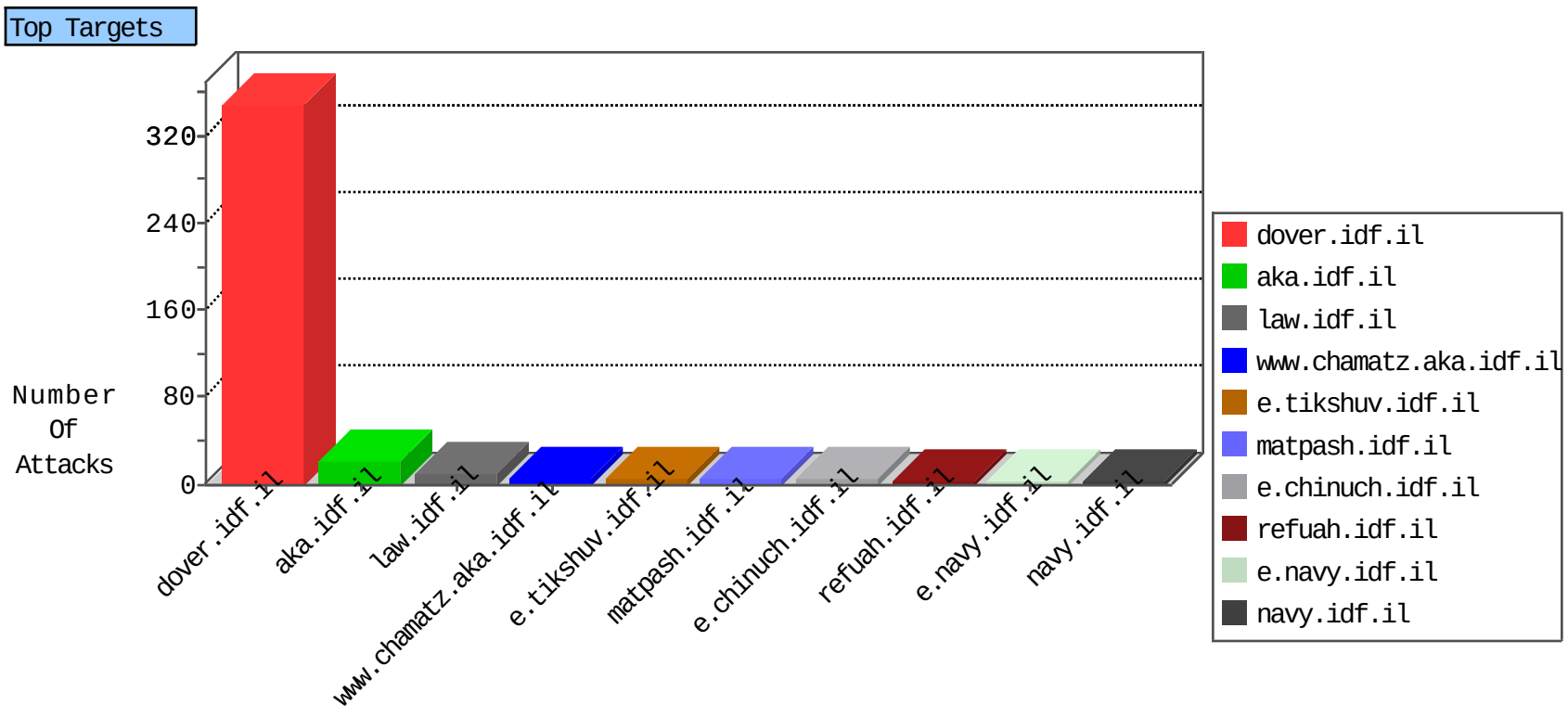
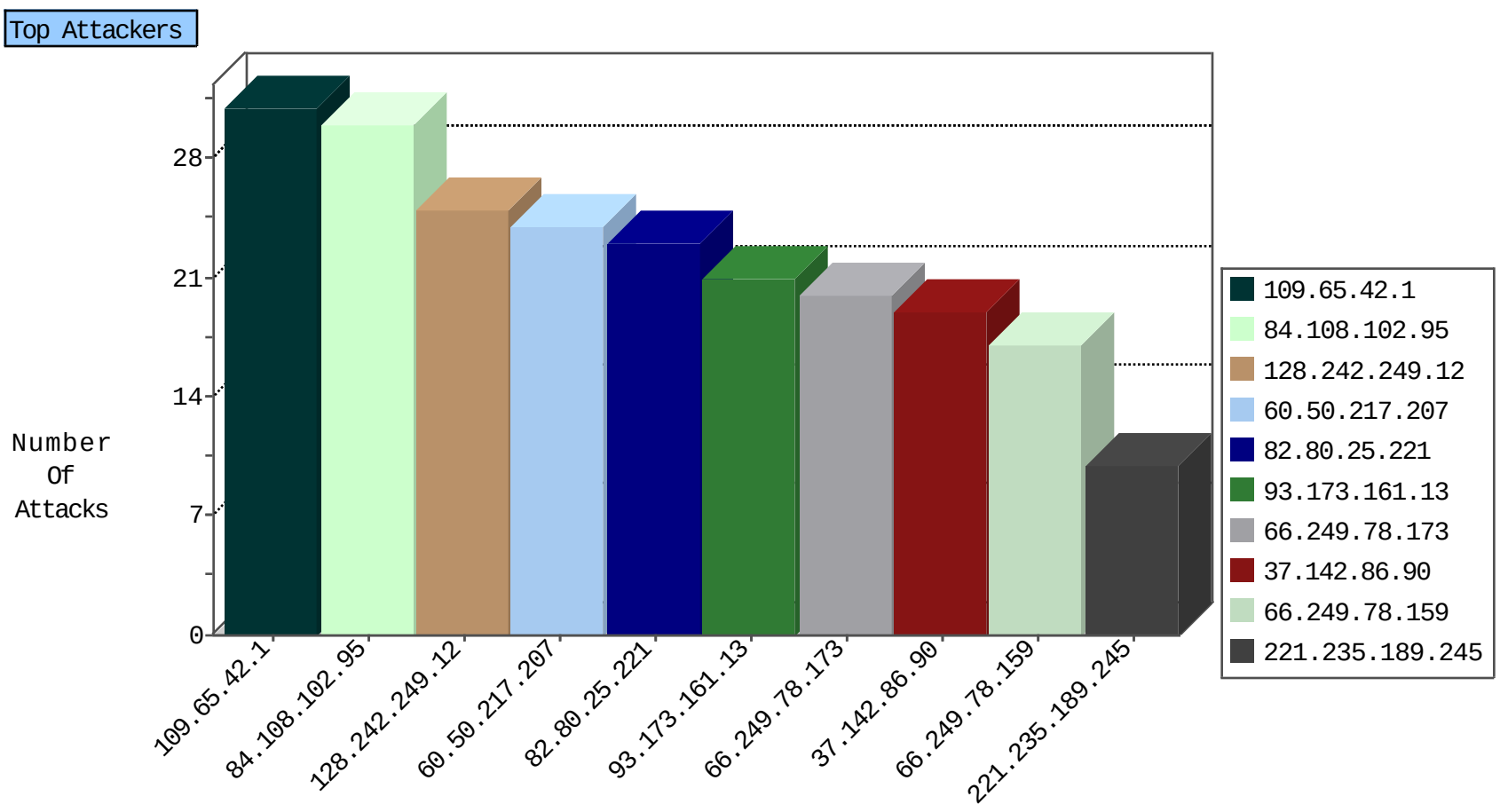
05-09-2015-05:03:00 to 05-09-2015-06:03:00

IDF Under Attack
05-09-2015-05:03:00





05-09-2015-05:03:00 to 05-09-2015-06:03:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.108	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	123
66.249.67.139	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	94
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
60.50.217.207	Malaysia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
104.192.0.20		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

05-09-2015-05:03:00 to 05-09-2015-06:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	25
71.6.165.200	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	2
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.121	e.navy.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1

05-09-2015-05:03:00 to 05-09-2015-06:03:00

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
61.240.144.65	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.31	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.190	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.66	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	United States	147.237.76.177	ncore.idf.il	ET DROP Dshield Block Listed Source	1
61.240.144.66	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
182.254.226.90	China	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
175.136.197.37	Malaysia	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
121.46.0.125	China	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
58.54.134.13	China	147.237.76.30	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
221.235.189.245	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
87.101.142.40	Saudi Arabia	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
8.29.144.205	United States	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
221.235.189.245	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.245	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.176	matpash.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
221.235.189.245	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.245	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
175.136.197.37	Malaysia	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.66	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
175.136.197.37	Malaysia	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.65	China	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
175.136.197.37	Malaysia	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.65	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
114.112.90.54	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
8.29.144.205	United States	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
221.235.189.245	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
87.101.142.40	Saudi Arabia	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.245	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
221.235.189.245	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

05-09-2015-05:03:00 to 05-09-2015-06:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
109.65.42.1	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	31
84.108.102.95	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
60.50.217.207	Malaysia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
93.173.161.13	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	21
37.142.86.90	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
82.80.25.221	Israel	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
24.193.76.103	United States	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	9
67.8.83.194	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
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
84.228.145.254	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
24.60.82.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
41.33.231.86	Egypt	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
66.249.64.178	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
157.55.39.162	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
217.33.206.131	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
93.173.253.127	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.64.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
149.88.25.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.228.145.254	Israel	147.237.77.216	dover.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	2
162.243.61.230	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.64.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
157.55.39.136	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
17.142.151.220	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.250.218.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
174.129.237.157	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
199.119.124.42	United States	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
184.105.139.71	United States	147.237.8.50	e.tikshuv.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1
37.142.121.152	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unexpected post SYN packet - RST or SYN expected	drop	drop	1
216.218.206.86	United States	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
27.45.196.14	China	147.237.77.176	matpash.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
66.249.64.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
188.138.1.218	Germany	147.237.8.50	e.tikshuv.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1
157.55.39.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
27.45.196.14	China	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
119.4.57.25	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
79.178.100.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
188.138.17.205	France	147.237.8.14	e.orchot.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.17.40.227	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
220.181.108.114	China	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
94.153.9.66	Ukraine	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il//templates/getfile/	Block	5
157.55.39.191	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.191	Block	3
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.136	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	2
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.162	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
213.251.182.103	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	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
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	2
166.216.157.119	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/templates/inner.asp	Block	1
63.141.249.155	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17436-en/dover.aspx/trackback/	Block	1
157.55.39.7	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.91	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/72199-he/maarachot.aspx	Block	1
171.37.221.116	China	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/faq.aspx	None	1
66.249.78.199	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-he/dover.aspx	Block	1
157.55.39.103	United States	147.237.76.30	himush.idf.il	Unknown Parameter PageNum in www.chimush.atal.idf.il/994-he/himush.aspx	None	1
66.249.78.73	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/announcements/2003/may/17.stm	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
66.249.79.193	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/edim/yoman/enlarge.asp	Block	1
66.249.64.244	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//sip_storage/files/3/68633...	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/doctrine/doctrine.stm	Block	1
157.55.39.123	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/contactus/pages/default.aspx	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-18115-he/dover.aspx	Block	1
27.45.196.14	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 27.45.196.14	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1065-he/kkkkkkk=5463f033kkkkkkk_5463f033	Block	1
157.55.39.143	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.64.245	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-10863-en/dover.aspx	Block	1
157.82.156.135	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/atar/	Block	1
27.45.196.14	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
180.76.5.155	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
157.55.39.161	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.79	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/261-6436-he/patzar.aspx	Block	1