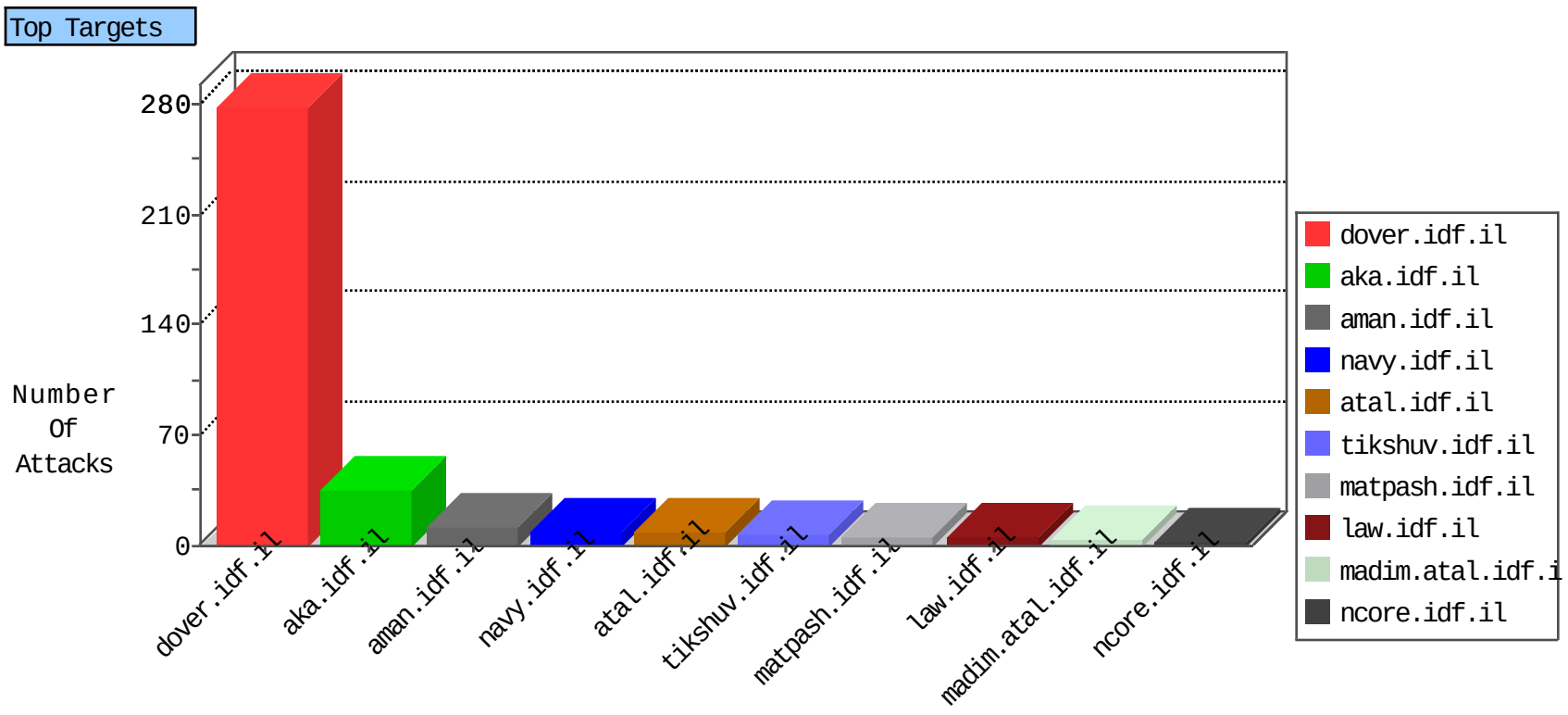
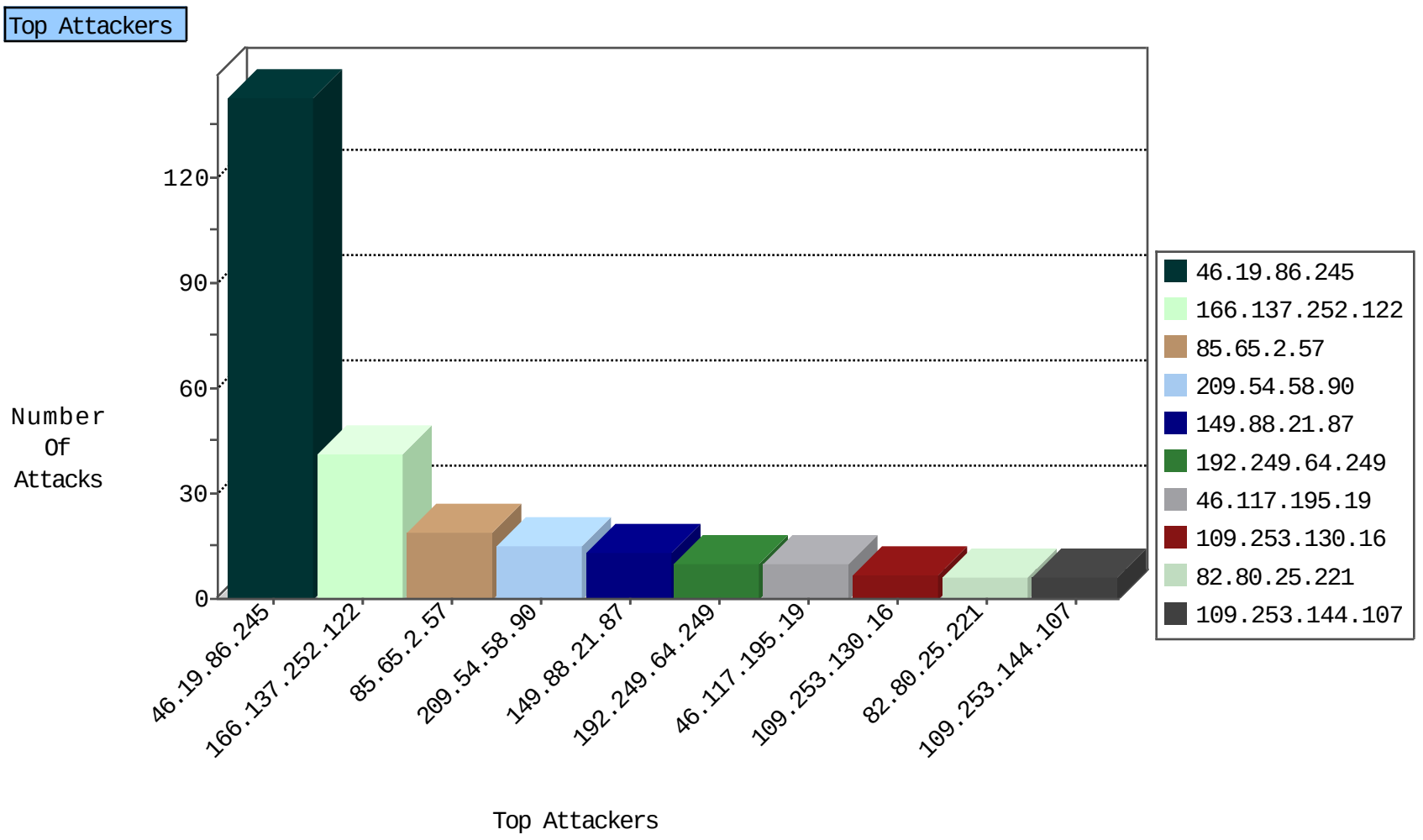
04-25-2015-00:03:03 to 04-25-2015-01:03:03

IDF Under Attack
04-25-2015-00:03:03

Top Targets



Top Attackers



04-25-2015-00:03:03 to 04-25-2015-01:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.100	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	393
220.181.108.165	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	383
46.117.195.19	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
66.249.65.171	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
193.242.218.6	Switzerland	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
36.47.136.230	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

04-25-2015-00:03:03 to 04-25-2015-01:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
89.139.31.120	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
85.25.43.94	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.148	gqcenter.aka.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	147.237.76.177	ncore.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
85.25.103.50	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.212	e.dover.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
198.20.70.114	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
84.108.16.175	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1

04-25-2015-00:03:03 to 04-25-2015-01:03:03

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	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
209.54.58.90	United States	147.237.0.34	tikshuv.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	3
209.54.58.90	United States	147.237.0.19	madim.atal.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	2
209.54.58.90	United States	147.237.0.15	kosher-kravi.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	2
66.249.78.204	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
66.249.75.94	United States	147.237.76.86	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.86	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.67	China	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.17.72	Russian Federation	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
149.210.182.186	Netherlands	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 4096	1
114.112.96.133	China	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.91.43	Israel	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
209.54.58.90	United States	147.237.0.17	m.my-kosher-kravi.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	1
193.107.17.72	Russian Federation	147.237.76.197	e.himush.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
149.210.182.186	Netherlands	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
82.166.91.43	Israel	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 4096	1

04-25-2015-00:03:03 to 04-25-2015-01:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.86.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	143
166.137.252.122	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
149.88.21.87	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
109.253.130.16	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
109.253.144.107	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.116.179.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
89.138.231.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
79.177.80.244	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
149.78.233.80	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.108.16.175	Israel	147.237.72.166	aka.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	2
157.55.39.178	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
85.64.219.192	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
64.236.82.70	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
85.72.40.4	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
125.209.235.185	Korea, Republic of	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
216.243.31.2	United States	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
176.58.78.176	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	1
92.247.181.29	Bulgaria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
188.165.15.13	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
77.126.212.156	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
176.58.77.63	Palestinian Territory, Occupied	147.237.77.176	matpash.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
85.65.2.57	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.65.2.57	Block	16
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	4
46.120.31.188	Israel	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
188.161.107.117	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en	Block	1
66.249.69.28	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
85.65.2.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/[object object]	Block	1
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1206-en/cogat.aspxcoordination	Block	1
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	1
209.54.58.90	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/cgi-bin/php	Block	1
37.212.201.56	Belarus	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/home/pniot.aspx	Block	1
84.108.16.175	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.75.39	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/m/	Block	1
188.165.15.94	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/61998	Block	1
66.249.69.76	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
89.139.31.120	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2003/january/16b.stm	Block	1
209.54.58.90	United States	147.237.0.34	tikshuv.idf.il	Access to: /cgi-bin/php	Block	1
157.55.39.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/122303-6.stm	Block	1
85.65.2.57	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request URL	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
209.54.58.90	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/cgi-bin/php	Block	1
66.249.69.76	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/1/1381.pdf	Block	1
89.169.43.217	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/	Block	1
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	1
209.54.58.90	United States	147.237.0.34	tikshuv.idf.il	Malformed URL http/1.1	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.121.193.253	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
85.65.2.57	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding www.aka.idf.il/main/giyus/function () { var c = math.round(this[2] / 100 * 255); if (this[1] == 0) { return [c, c, c]; } else { var a = this[0] r 360; var e = a e 60; v math.round((this[2] * (100 - this[1])) / 10000 * 255); var d = math.round((this[2] * (6000 - this[1] * e)) / 600000 * 255); var b = math.round((this[2] * (6000 - this[1] * (60 - e))) / 600000 * 255); switch (math.floor(a / 60)) { case 0: return [c, b, g];	Block	1
66.249.75.54	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
209.54.58.90	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Malformed URL from 209.54.58.90	Block	1
2.92.82.75	Russian Federation	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/163-6958-en/patzar.aspx	Block	1
143.85.71.26	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
77.126.38.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/iaf/iaf5-2.stm	Block	1
209.54.58.90	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
180.76.4.205	China	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on 147.237.0.34//	Block	1
66.249.65.192	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19075-he/dover.aspx	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
209.54.58.90	United States	147.237.0.19	madim.atal.idf.il	Malformed URL http/1.1	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/iaf/iaf5.stm	Block	1
37.140.141.27	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	1
144.76.15.235	Germany	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
81.52.143.19	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/main.stm	Block	1
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1