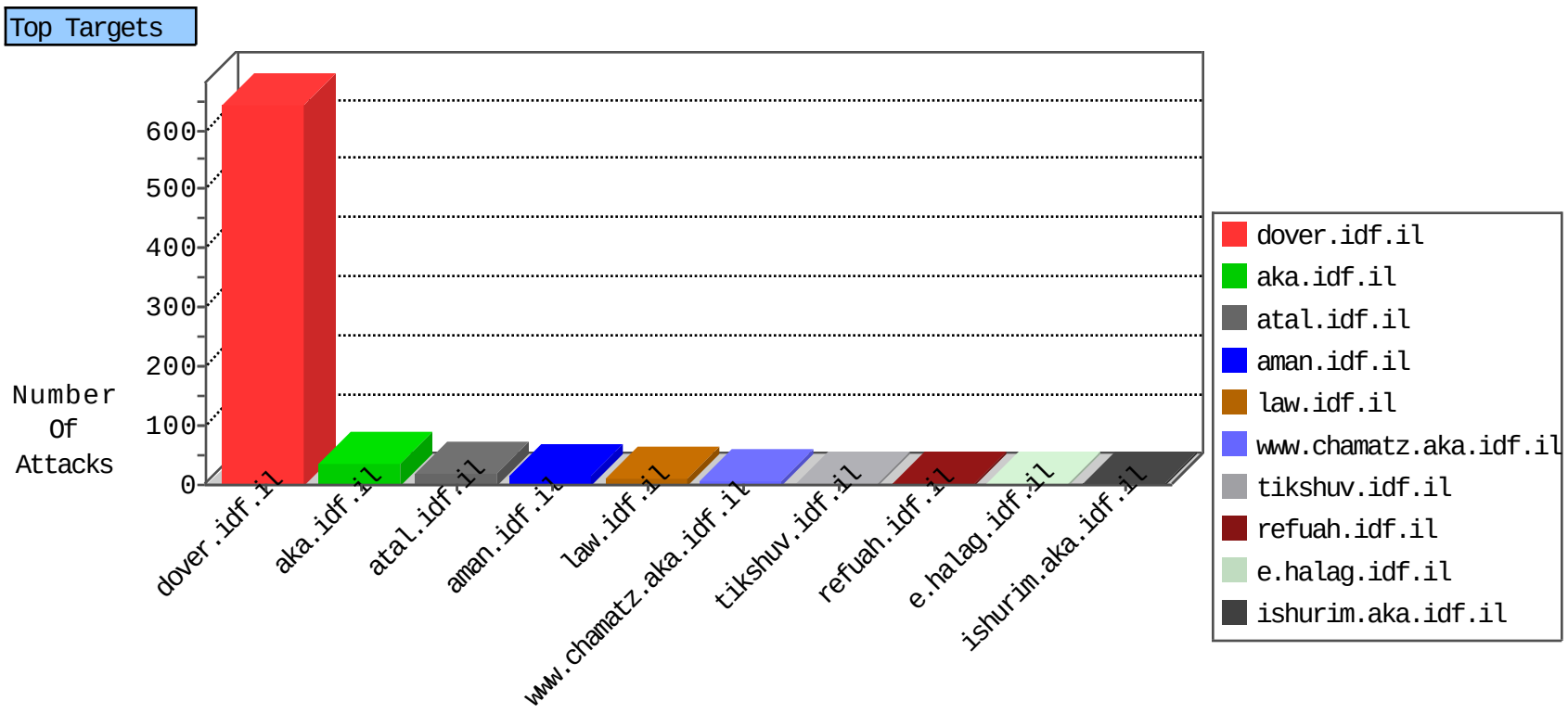
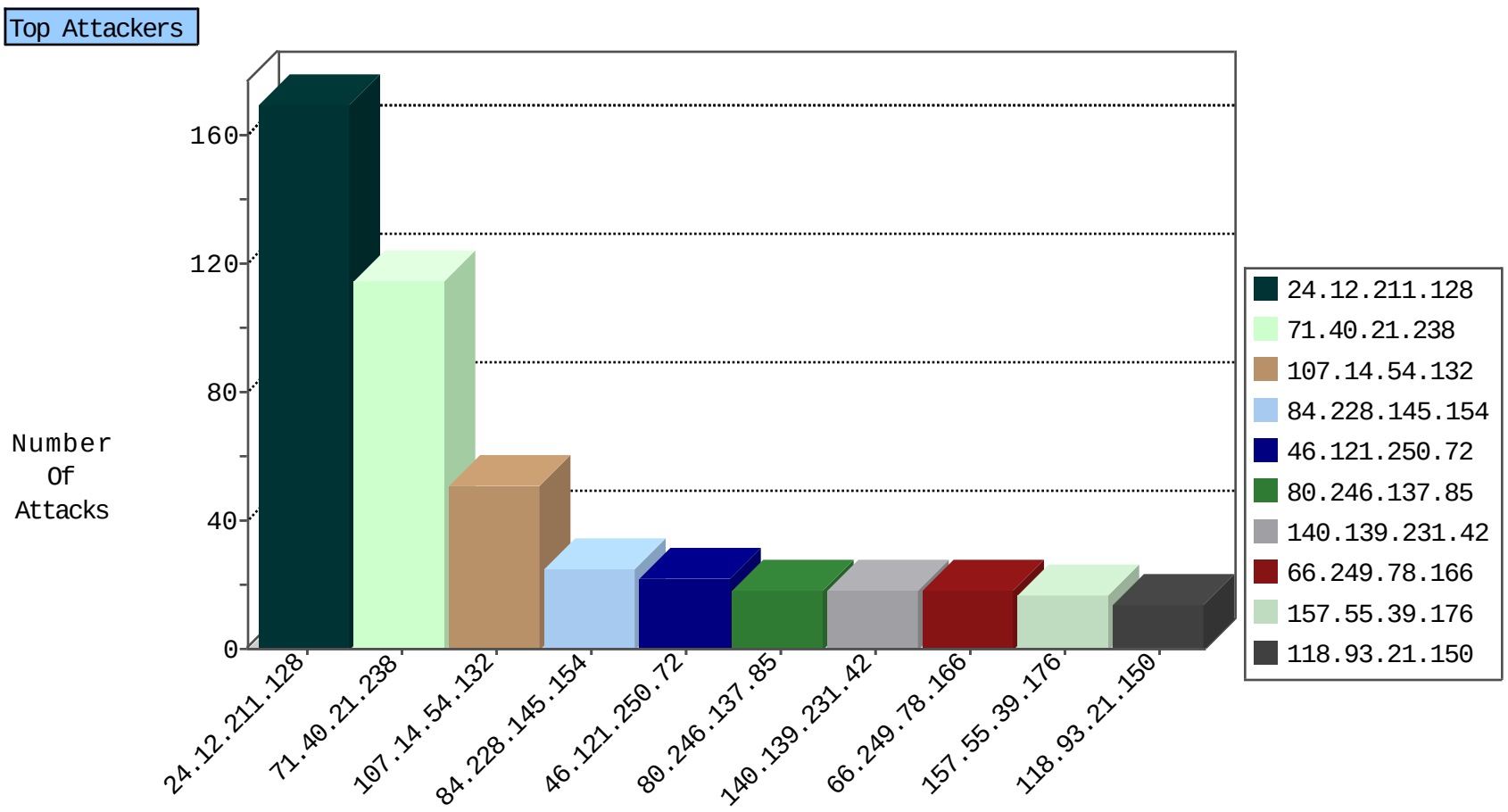
04-29-2015-04:03:09 to 04-29-2015-05:03:09

IDF Under Attack
04-29-2015-04:03:09

Top Targets



Top Attackers



04-29-2015-04:03:09 to 04-29-2015-05:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.67.116	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1472
93.172.27.159	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
220.181.108.182	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	60
220.181.108.155	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	53
66.249.67.84	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

04-29-2015-04:03:09 to 04-29-2015-05:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
41.185.12.165	South Africa	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
46.116.211.238	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
114.32.178.177	Taiwan	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4
46.121.250.72	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	3
85.17.242.234	Netherlands	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	3
198.20.69.98	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	2
66.240.192.138	United States	147.237.8.14	e.orchot.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
71.6.165.200	United States	147.237.76.176	test.ncore.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
85.25.103.50	Germany	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.0.34	tikshuv.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
71.6.165.200	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
94.23.6.131	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.76.86	navy.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
71.6.165.200	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.233	atal.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
62.210.97.48	France	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	1
71.6.165.200	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1

04-29-2015-04:03:09 to 04-29-2015-05:03:09

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
212.76.108.157	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.67.84	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.92	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.78	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
213.210.205.2	Saudi Arabia	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
178.19.107.114	Poland	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.8.164	France	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.66	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
213.210.205.2	Saudi Arabia	147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
62.210.8.164	France	147.237.72.217	e.idf.il	ET SCAN NMAP -sS window 1024	1
8.29.144.205	United States	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 3072	1

04-29-2015-04:03:09 to 04-29-2015-05:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
24.12.211.128	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	170
71.40.21.238	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	115
107.14.54.132	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	51
84.228.145.154	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
140.139.231.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
157.55.39.176	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
107.14.54.142	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
118.93.21.150	New Zealand	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
46.121.250.72	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	12
179.111.203.100	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
37.26.148.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
65.25.242.30	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
82.119.4.16	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
77.127.188.214	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.78.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
87.68.26.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.121.250.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
70.49.188.85	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
85.17.242.234	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.253.128.48	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.178.8.36	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
188.138.17.205	France	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
2.54.7.185	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
68.192.83.66	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
88.198.25.217	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
77.125.119.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
188.166.99.132	Russian Federation	147.237.8.50	e.tikshuv.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
66.249.78.109	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
98.245.100.137	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.121.250.72	Israel	147.237.77.234	halag.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	2
109.64.26.146	Israel	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	2
66.249.82.202	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
212.235.103.203	Israel	147.237.72.167	ishurim.aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
176.12.148.66	Israel	147.237.0.15	kosher-kravi.idf.i	Invalid ACK number	Bad TCP sequence	monitor	1
31.172.30.2	Switzerland	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.64.28	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

04-29-2015-04:03:09 to 04-29-2015-05:03:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.28.105.11	Czech Republic	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.28.105.11	Block	4
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
100.2.135.132	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	Block	2
188.138.17.205	France	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
78.46.51.124	Germany	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.78.21	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/m/	Block	1
66.249.64.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
157.55.39.237	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//938-he/refuah.aspx	Block	1
66.249.67.54	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
198.204.252.19	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
46.28.105.11	Czech Republic	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/test/wp-admin/	Block	1
78.47.218.149	Germany	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-he/dover.aspx	Block	1
66.249.64.66	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
178.137.166.68	Ukraine	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/2004/january/0128-1.stm	Block	1
66.249.67.62	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/261-6570-he/patzar.aspx	Block	1
198.204.252.19	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
46.121.220.110	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20297-he/idfgdover.aspx	Block	1
66.249.64.73	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//console/core/doc_mgr/undefined	Block	1
180.76.5.60	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ns-welcome.stm	Block	1
69.118.64.11	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/1/	Block	1
66.249.67.70	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-4906-he/patzar.aspx	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
46.121.250.72	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
109.67.23.224	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.64.77	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il//console/core/doc_mgr/undefined	Block	1
182.53.30.16	Thailand	147.237.77.216	dover.idf.il	Unknown HTTP Request Method COOK in URL www.idf.il/1283-17607-en/dover.aspx	Block	1
69.162.72.162	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17155-en/dover.aspx/trackback/	Block	1
66.249.67.128	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1312-he/refuah.aspx	Block	1
217.172.179.75	Germany	147.237.72.167	ishurim.aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.64.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-18296-en/dover.aspx	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	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
66.249.64.77	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1

04-29-2015-04:03:09 to 04-29-2015-05:03:09