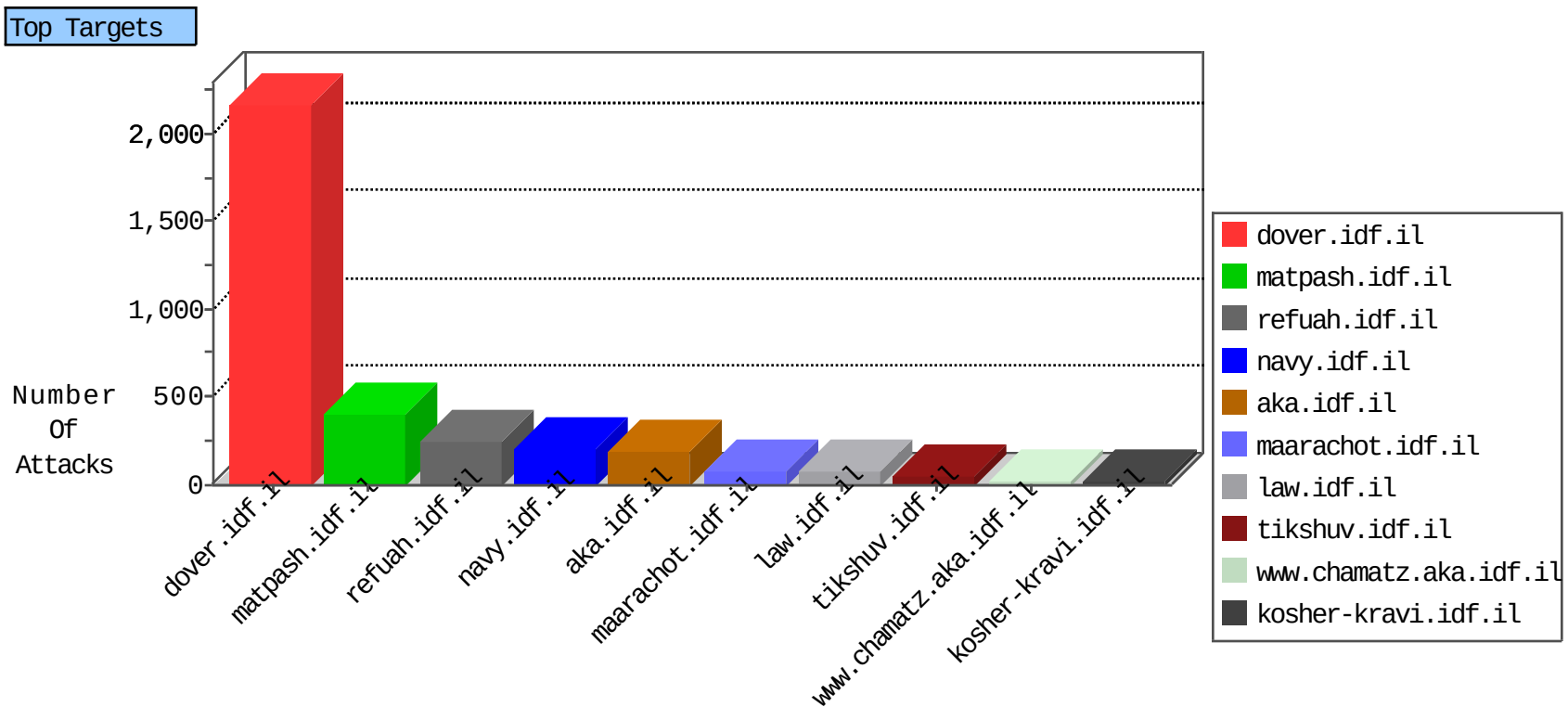
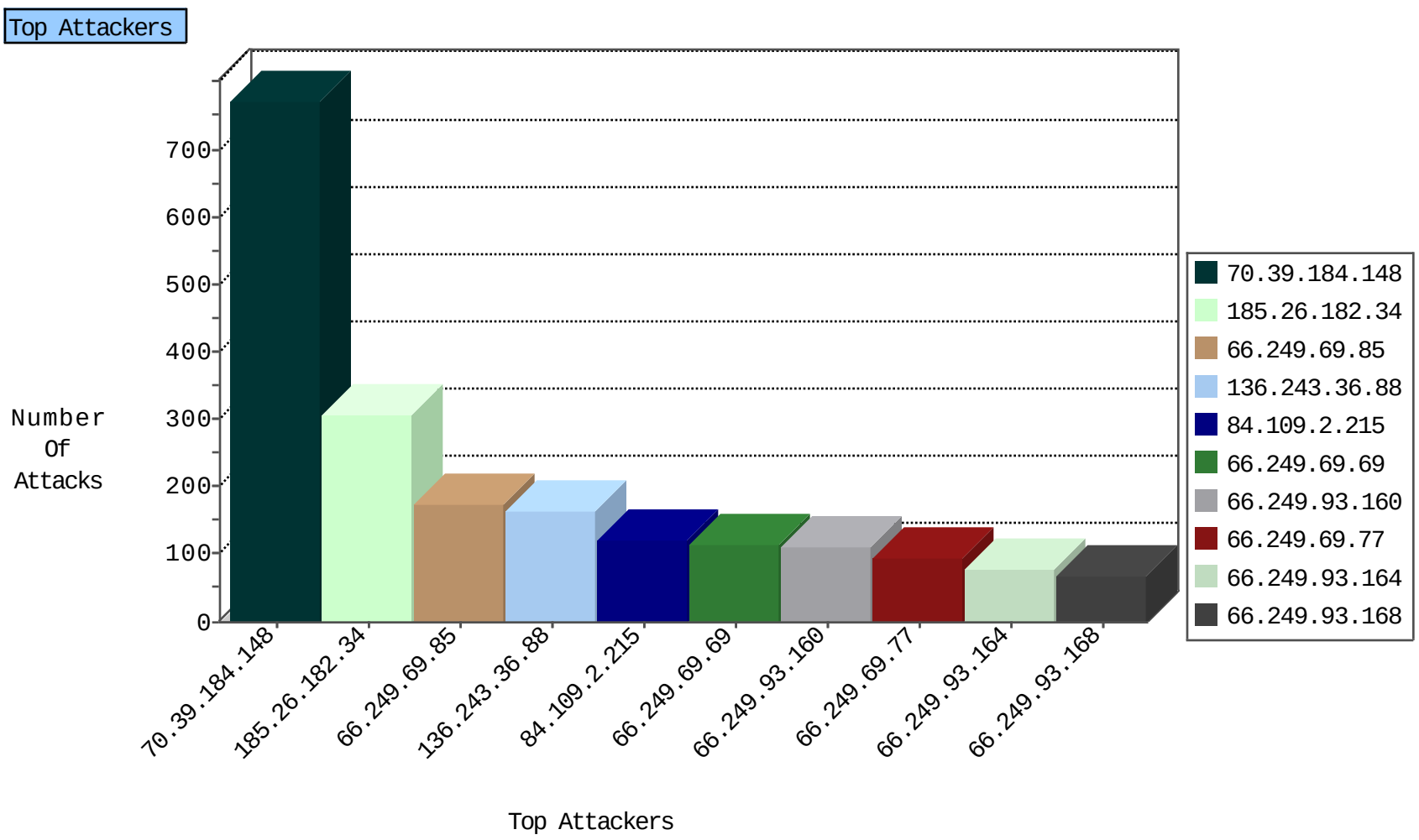
04-11-2015-03:03:00 to 04-11-2015-04:03:00

IDF Under Attack
04-11-2015-03:03:00





04-11-2015-03:03:00 to 04-11-2015-04:03:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.69.85	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	174
66.249.69.69	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	113
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	111
66.249.69.77	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	93
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	79
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	68
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	63
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	62
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	53
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	43
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	31
66.249.78.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	31
66.249.78.111	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	30
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	27
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	25
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	24
66.249.69.95	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	24
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	23
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	22
66.249.67.100	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	16
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	16
66.249.78.104	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	15
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.67.108	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	14
66.249.69.79	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	14
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	14
66.249.69.105	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ip_Web_In	drop	13
149.78.243.43	United States	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	13
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	12
66.249.78.74	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.69.87	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	11
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	10
66.249.67.34	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	9
66.249.78.79	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	9
66.249.67.42	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	9
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	9
66.249.89.103	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	9
66.249.67.50	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	9
66.249.67.3	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.73.201	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.64.150	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	8
66.249.64.142	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	8
66.249.64.92	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	8
66.249.69.117	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ip_Web_In	drop	7
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
70.39.184.148	Satellite Provider	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	6
66.249.67.99	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	6
66.249.80.83	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.67.147	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5

04-11-2015-03:03:00 to 04-11-2015-04:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
41.129.121.166	Egypt	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
93.120.27.62	Romania	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
105.102.70.230	Algeria	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

04-11-2015-03:03:00 to 04-11-2015-04:03:00

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	24
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
105.102.70.230	Algeria	147.237.77.216	dover.idf.il	SERVER-WEBAPP encoded cross site scripting HTML Image tag attempt	2
61.175.255.61	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -f -sS	1
198.23.140.18	United States	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 4096	1
113.21.226.56	New Zealand	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.56.231	Netherlands	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
80.55.55.59	Poland	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
61.240.144.67	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.175.255.61	China	147.237.76.201	e.atal.idf.il	ET SCAN NMAP -sS window 2048	1
195.154.225.28	France	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
193.107.17.72	Russian Federation	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
105.102.70.230	Algeria	147.237.77.216	dover.idf.il	SQL Injection - Select From	1
94.102.56.231	Netherlands	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
80.55.55.59	Poland	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.64	China	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1

04-11-2015-03:03:00 to 04-11-2015-04:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
70.39.184.148	Satellite Provider	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	766
185.26.182.34	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	307
136.243.36.88	Germany	147.237.76.42	refuah.idf.il	SAM rule	drop	drop	104
84.109.2.215	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	66
84.109.2.215	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	49
85.65.101.18	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
70.75.186.236	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
2.54.32.197	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
109.253.146.21	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	30
98.220.218.102	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
136.243.36.88	Germany	147.237.72.166	aka.idf.il	SAM rule	drop	drop	22
136.243.36.88	Germany	147.237.77.176	matpash.idf.il	SAM rule	drop	drop	21
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
136.243.36.88	Germany	147.237.72.167	ishurim.aka.idf.i	SAM rule	drop	drop	16
109.253.145.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
84.211.16.251	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
80.246.133.63	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
213.57.147.5	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
157.55.39.114	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
105.102.70.230	Algeria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
220.255.1.163	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
220.255.1.114	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
69.171.246.116	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
188.165.15.241	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
220.255.1.123	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
105.102.70.230	Algeria	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
69.171.246.115	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
220.255.1.126	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
220.255.1.133	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
173.252.81.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
220.255.1.135	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
220.255.1.160	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
220.255.1.110	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
220.255.1.142	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
220.255.1.116	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
38.98.9.76	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
220.255.1.103	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
220.255.1.153	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4

04-11-2015-03:03:00 to 04-11-2015-04:03:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
105.102.70.230	Algeria	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	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
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0713-1.stm	Block	1
31.170.118.97	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/russian/main.stm	Block	1
188.143.232.40	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.40	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/2/62532.pdfg2=whvq9jgvov3igm-oflegda	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/pakar5.stm	Block	1
31.184.195.166	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
188.143.232.40	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
157.55.39.121	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.121.247.55	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
188.165.15.10	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-5846-he/patzar.aspx	Block	1
84.109.2.215	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
176.241.87.44	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/qar/	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
198.20.69.74	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
84.109.179.49	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
188.143.232.40	Russian Federation	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/news/news.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1

04-11-2015-03:03:00 to 04-11-2015-04:03:00