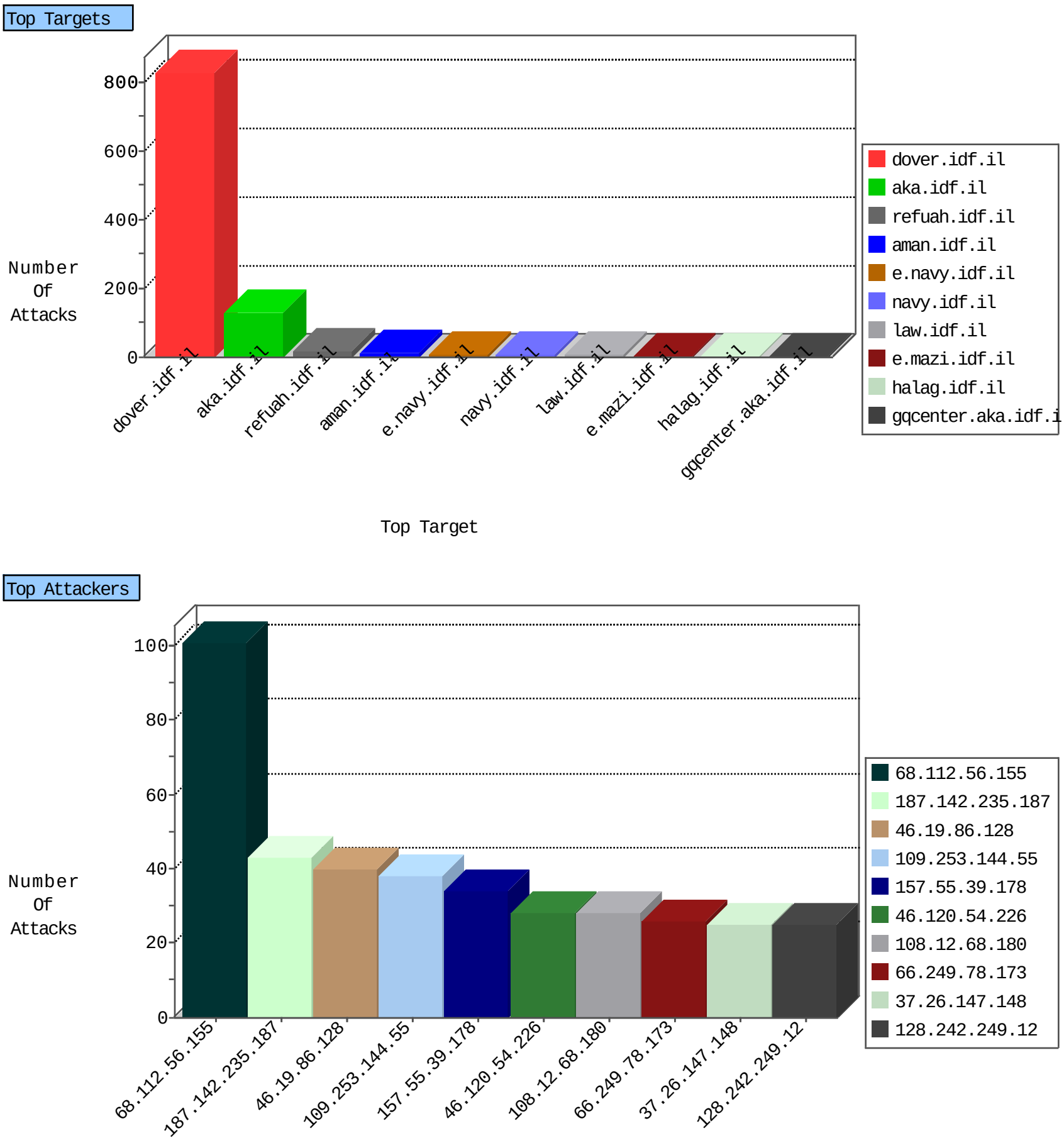
04-30-2015-06:03:08 to 04-30-2015-07:03:08

IDF Under Attack
04-30-2015-06:03:08



04-30-2015-06:03:08 to 04-30-2015-07:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	346
109.253.135.254	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
37.26.147.148	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	27
109.253.140.161	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	12
87.68.254.57	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
66.249.64.61	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
77.127.84.236	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.52.11.119	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
27.254.96.52	Thailand	147.237.72.217	e.idf.il	JLM_Purple_Con_Limit_Http	drop	1
195.37.190.86	Germany	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
66.249.67.84	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	1
27.254.96.52	Thailand	147.237.77.19	law-forum.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
195.37.190.86	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

04-30-2015-06:03:08 to 04-30-2015-07:03:08

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
37.26.147.198	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
66.240.236.119	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.148	gqcenter.aka.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
71.6.135.131	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.86	navy.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
66.240.236.119	United States	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
71.6.135.131	United States	147.237.72.167	ishurim.aka.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
71.6.167.142	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1

04-30-2015-06:03:08 to 04-30-2015-07:03:08

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
66.249.67.100	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
91.224.132.118	Russian Federation	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	Turkey	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.42	refuah.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
218.77.79.43	China	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
216.251.24.119	United States	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
91.238.134.92	Poland	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
91.145.45.76	Sweden	147.237.77.121	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.77.216	dover.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
218.77.79.43	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
61.183.128.6	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
216.251.24.119	United States	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1

04-30-2015-06:03:08 to 04-30-2015-07:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
68.112.56.155	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	98
187.142.235.187	Mexico	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	43
46.19.86.128	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	40
109.253.144.55	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
157.55.39.178	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	32
46.120.54.226	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
108.12.68.180	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	22
52.8.111.241	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
37.26.147.148	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
79.179.143.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
109.253.138.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
107.170.181.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
37.26.147.198	Israel	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	12
66.249.64.72	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
52.8.111.225	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
184.77.38.146	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
98.165.207.166	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
5.22.132.65	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
37.26.147.198	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
5.22.132.87	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	9
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.64.76	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	8
87.68.254.57	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
46.19.86.146	Israel	147.237.76.42	refuah.idf.i	Invalid ACK number	Bad TCP sequence	monitor	8
94.159.153.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
216.223.27.61	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	7
190.139.144.120	Argentina	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
85.250.61.43	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	6
193.34.57.101	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
144.132.83.63	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
85.250.61.43	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
2.54.142.135	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
223.132.125.70	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
198.251.58.183	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
84.111.7.79	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.86.206	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
109.253.147.106	Israel	147.237.76.42	refuah.idf.i	SYN retransmit with different window scale	Bad TCP sequence	monitor	4
157.55.39.3	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
37.26.148.203	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
109.160.249.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.86	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
91.145.45.76	Sweden	147.237.77.121	e.navy.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	4
31.186.228.59	United Kingdom	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4

04-30-2015-06:03:08 to 04-30-2015-07:03:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
157.55.39.178	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
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.66.121.237	Denmark	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 77.66.121.237	Block	2
184.105.247.195	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
31.193.51.84	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/library/manage/resource/getfilecontent.hh.asp	Block	1
79.177.102.51	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.75.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/999-he/atal.aspx	Block	1
123.24.105.61	Vietnam	147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.79.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.47	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/mod	Block	1
37.26.147.172	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.65.221.186	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.78.44	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/m/	Block	1
157.55.39.217	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/pdf/files/5/112435.pdf).	Block	1
142.54.161.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17055-en/dover.aspx/trackback/	Block	1
70.167.8.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0123-2.stm	Block	1
54.204.20.250	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.8	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.173.34.63	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19748-he/idfgdover.aspx	Block	1
172.252.82.198	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
149.88.70.110	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
54.215.88.171	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
108.41.7.127	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0212-2.stm	Block	1
180.76.4.220	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.64.29	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/m/	Block	1
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.147.106	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1

04-30-2015-06:03:08 to 04-30-2015-07:03:08