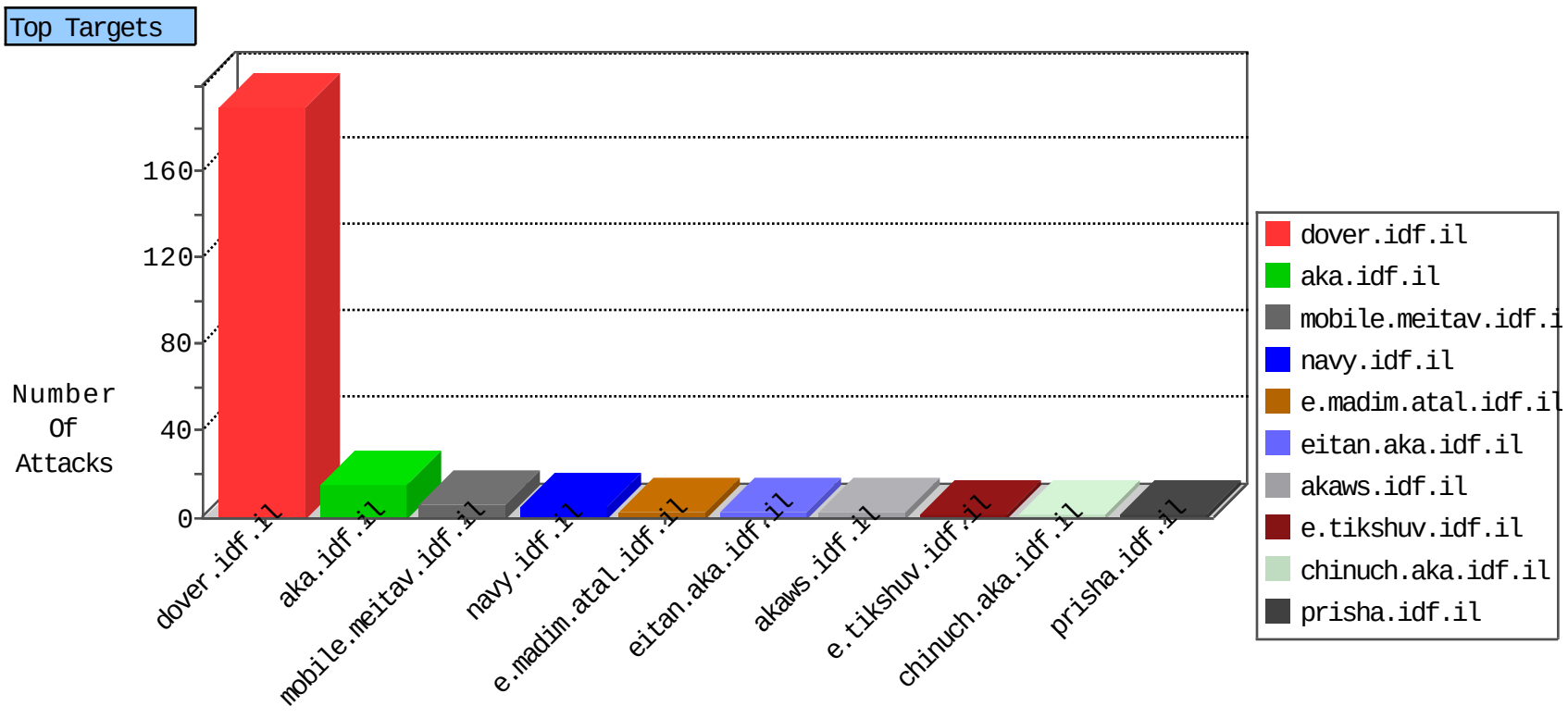
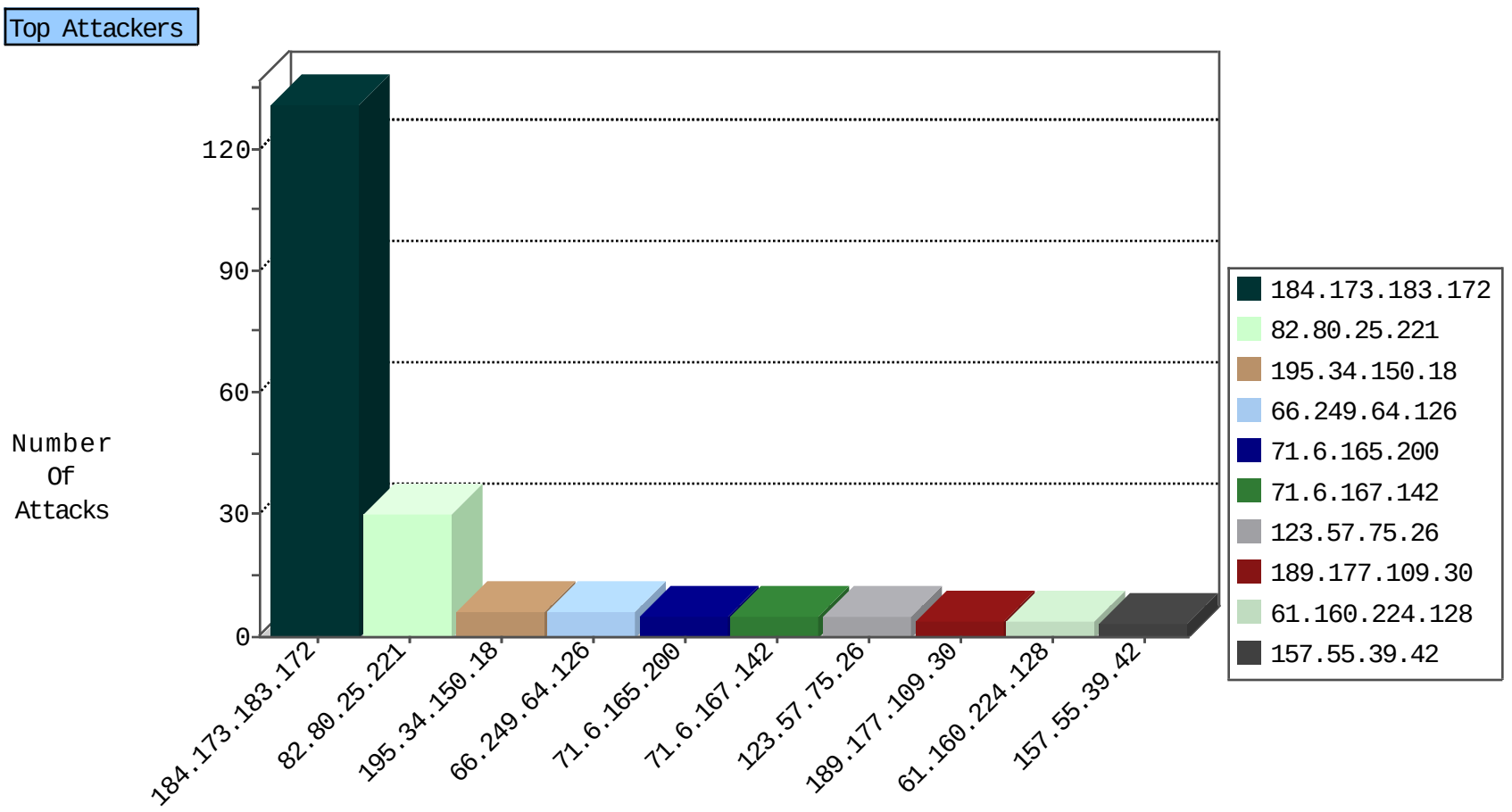
04-01-2015-05:03:09 to 04-01-2015-06:03:09

IDF Under Attack
04-01-2015-05:03:09

Top Targets



Top Attackers



04-01-2015-05:03:09 to 04-01-2015-06:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
189.177.109.30	Mexico	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	4
178.162.201.166	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
49.147.58.147	Philippines	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
107.154.64.10	United States	147.237.76.199	e.nakchal.idf.il	L4 Source or Dest Port Zero	drop	1
124.232.142.220	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

04-01-2015-05:03:09 to 04-01-2015-06:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	131
168.1.75.18	Switzerland	147.237.72.166	aka.idf.il	2023: HTTP: Cross Site Scripting in GET Request	Block	2
71.6.165.200	United States	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.243	mobile.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.19	madim.atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.176	test.ncore.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
71.6.167.142	United States	147.237.0.200	m4u.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	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1

04-01-2015-05:03:09 to 04-01-2015-06:03:09

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	30
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
89.248.162.228	Netherlands	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.93	Netherlands	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
123.57.75.26	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
123.57.75.26	China	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
123.57.75.26	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
208.124.237.146	Canada	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
61.160.224.128	China	147.237.76.44	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.76.86	navy.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
128.61.240.66	United States	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
123.57.75.26	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
123.57.75.26	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1

04-01-2015-05:03:09 to 04-01-2015-06:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.64.126	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
207.46.13.112	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
157.55.39.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
203.127.96.217	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
71.6.216.51	United States	147.237.77.61	e.cogat.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
71.6.216.42	United States	147.237.76.196	e.sviva.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
178.79.184.233	United Kingdom	147.237.76.200	eitan.aka.idf.il		drop	drop	1
71.6.216.49	United States	147.237.8.27	e.madim.atal.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.85.183	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
71.6.216.53	United States	147.237.0.35	akaws.idf.il		drop	drop	1
71.6.216.45	United States	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
184.105.139.124	United States	147.237.0.33	idf.il		drop	drop	1
71.6.216.49	United States	147.237.76.147	chinuch.aka.idf.il		drop	drop	1
46.19.85.216	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
73.205.190.31	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
71.6.216.46	United States	147.237.76.200	eitan.aka.idf.il		drop	drop	1
188.120.148.187	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
71.6.216.50	United States	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.85.216	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
146.185.239.104	Russian Federation	147.237.76.196	e.sviva.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
71.6.216.47	United States	147.237.72.217	e.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
188.138.17.205	France	147.237.8.50	e.tikshuv.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
71.6.216.51	United States	147.237.0.33	idf.il		drop	drop	1
71.6.216.47	United States	147.237.76.201	e.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1

04-01-2015-05:03:09 to 04-01-2015-06:03:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
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
98.213.218.12	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	2
149.78.215.29	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chinuch	Block	2
207.46.13.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/bagatz_sarbanim.stm	Block	1
84.229.199.186	Israel	147.237.72.166	aka.idf.il	Distributed Unknown Parameter on www.aka.idf.il/main/sachar/ parameter __EVENTVALIDATION	None	1
66.249.64.128	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1531-12946-he/dover.aspx	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0128-3.stm	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0113-1.stm	Block	1
46.19.85.183	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
216.218.206.67	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
84.229.199.186	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.64.150	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arafat/english/main_index.stm	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/military-police	Block	1
50.16.14.36	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
87.69.109.202	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/home.aspx	None	1
66.249.75.13	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluim/templates/hom.asp	Block	1
157.55.39.130	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
74.82.47.3	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
54.166.233.84	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
66.249.75.109	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.2	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
79.176.149.248	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
54.221.198.105	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.asp	Block	1
66.249.78.65	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1

04-01-2015-05:03:09 to 04-01-2015-06:03:09