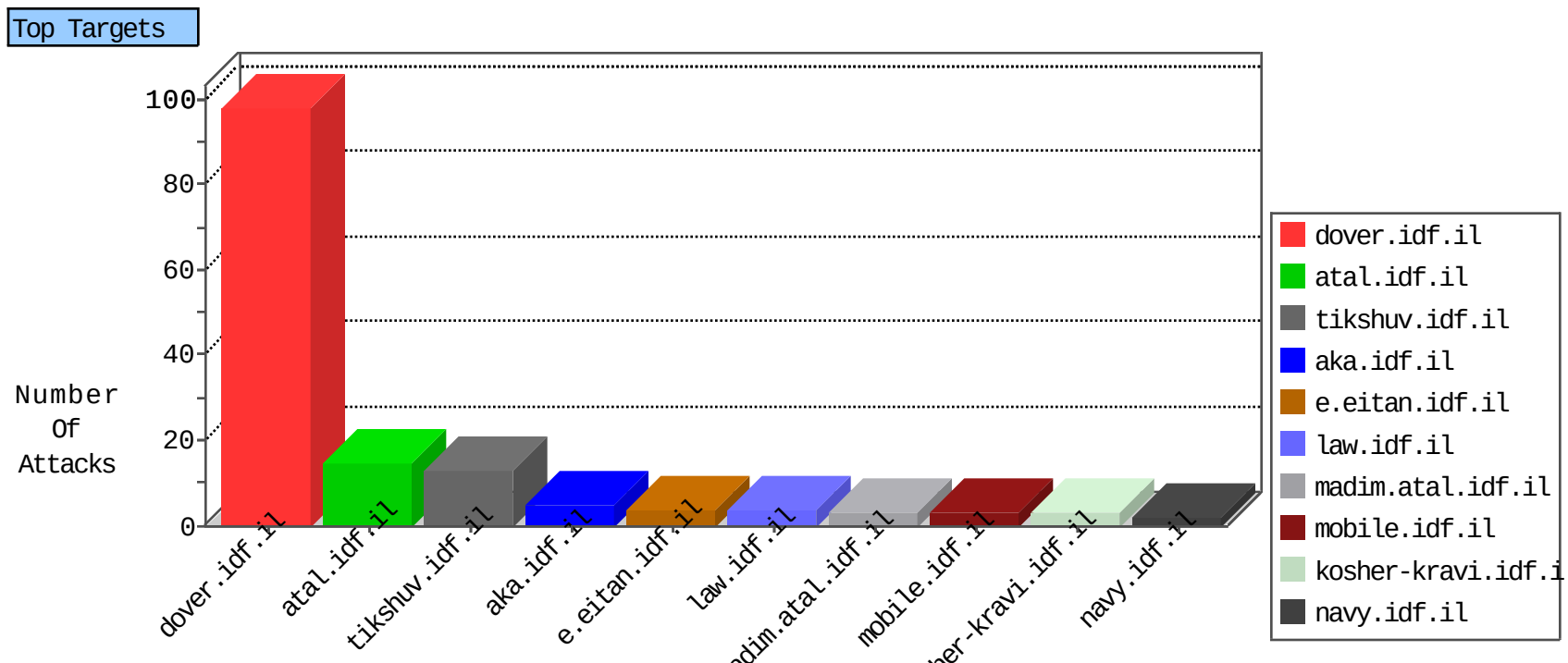
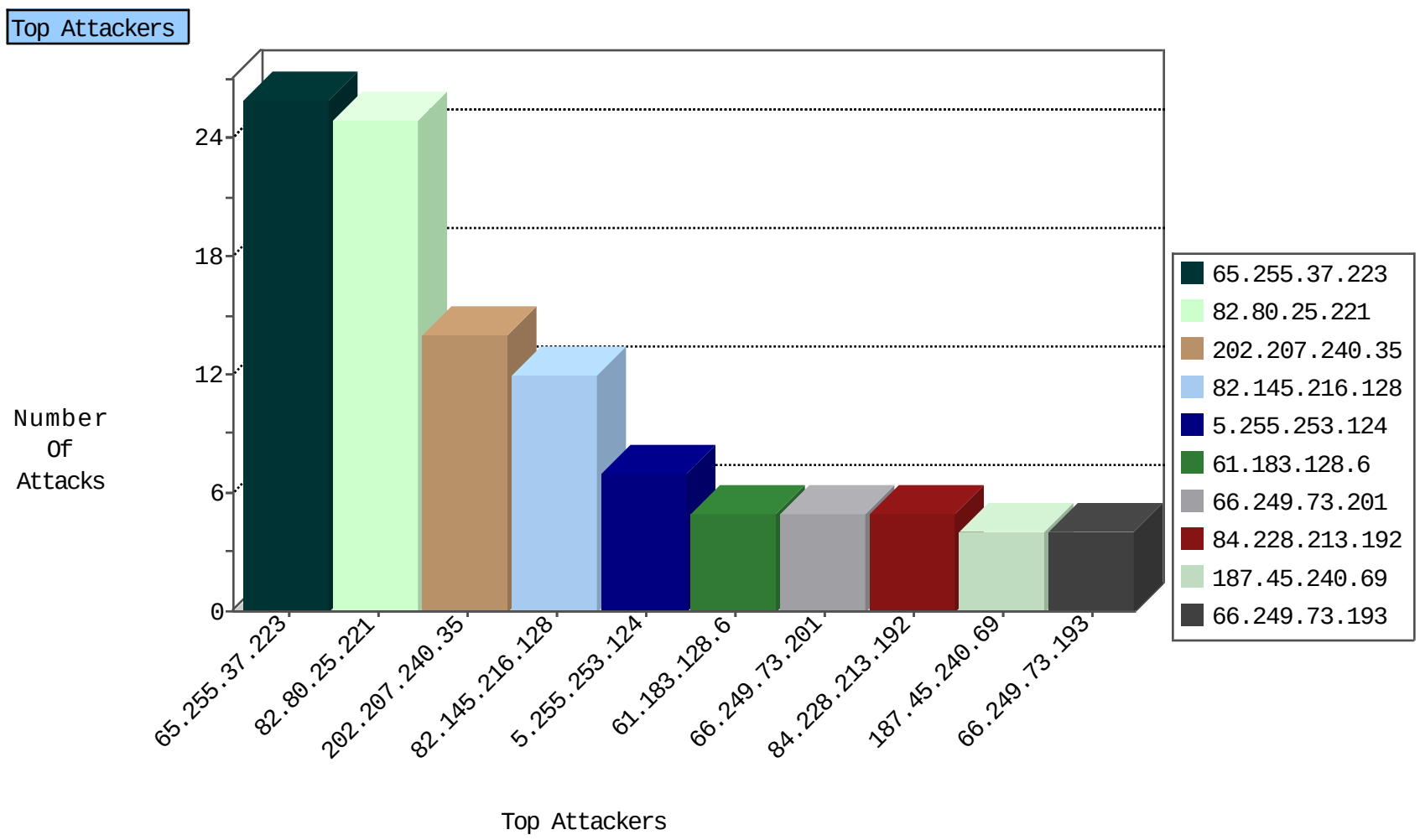
04-25-2015-06:03:03 to 04-25-2015-07:03:03

IDF Under Attack
04-25-2015-06:03:03

Top Targets



Top Attackers



04-25-2015-06:03:03 to 04-25-2015-07:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
59.147.200.207	Japan	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
195.37.190.86	Germany	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1

04-25-2015-06:03:03 to 04-25-2015-07:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
185.32.177.43	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.59.254.88	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
198.20.69.98	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

04-25-2015-06:03:03 to 04-25-2015-07:03:03

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	25
202.207.240.35	China	147.237.0.34	tikshuv.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
61.183.128.6	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.75.68	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.183.128.6	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
202.207.240.35	China	147.237.0.15	kosher-kravi.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	1
46.130.112.242	Armenia	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
184.63.17.245	United States	147.237.77.216	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	1
46.130.112.242	Armenia	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
114.112.96.133	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
212.47.236.90	France	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
212.47.236.90	France	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
202.207.240.35	China	147.237.0.19	madim.atal.idf.il	ET WEB_SERVER Possible CVE-2014-6271 Attempt in Headers	1
60.18.162.244	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.130.112.242	Armenia	147.237.8.45	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
114.112.96.133	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
91.238.134.92	Poland	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
212.47.236.90	France	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1

04-25-2015-06:03:03 to 04-25-2015-07:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
65.255.37.223	Satellite Provider	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	26
82.145.216.128	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
84.228.213.192	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	4
207.241.226.169	United States	147.237.72.166	aka.idf.il	SAM rule	drop	drop	1

04-25-2015-06:03:03 to 04-25-2015-07:03:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	7
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	5
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	4
202.207.240.35	China	147.237.0.34	tikshuv.idf.il	Multiple URL worm attacks from 202.207.240.35	Block	4
187.45.240.69	Brazil	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 187.45.240.69	Block	3
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	3
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	Multiple Unauthorized URL Access from 68.180.228.117	Block	2
180.76.4.78	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
188.165.15.13	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1008-2.stm	Block	1
157.55.39.8	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.52	Block	1
184.63.17.245	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clientscripts/{0}	Block	1
84.228.213.192	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.73.223	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/navmenu/	Block	1
202.207.240.35	China	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/cgi-bin/contact.cgi	Block	1
157.55.39.59	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/course_photos.asp	Block	1
66.249.69.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
207.46.13.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0115-2.stm	Block	1
91.200.12.22	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11845-en/dover.aspx/trackback/	Block	1
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.78.204	Block	1
202.207.240.35	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/cgi-bin/env.cgi	Block	1
157.55.39.115	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/031604-2.stm	Block	1
217.12.202.39	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
187.45.240.69	Brazil	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/wp-admin/	Block	1
135.23.110.73	Canada	147.237.77.233	atal.idf.il	E-mail collector robots 14	Block	1
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
202.207.240.35	China	147.237.0.34	tikshuv.idf.il	Access to: /cgi-bin/contact.cgi	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/barak/barak.stm	Block	1
69.162.153.76	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/english/default.stm	Block	1
221.180.17.227	China	147.237.0.34	tikshuv.idf.il	Malformed URL http/1.1	Block	1
188.138.17.205	France	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/	Block	1
135.23.110.73	Canada	147.237.77.233	atal.idf.il	eMail Hoarding	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1

04-25-2015-06:03:03 to 04-25-2015-07:03:03