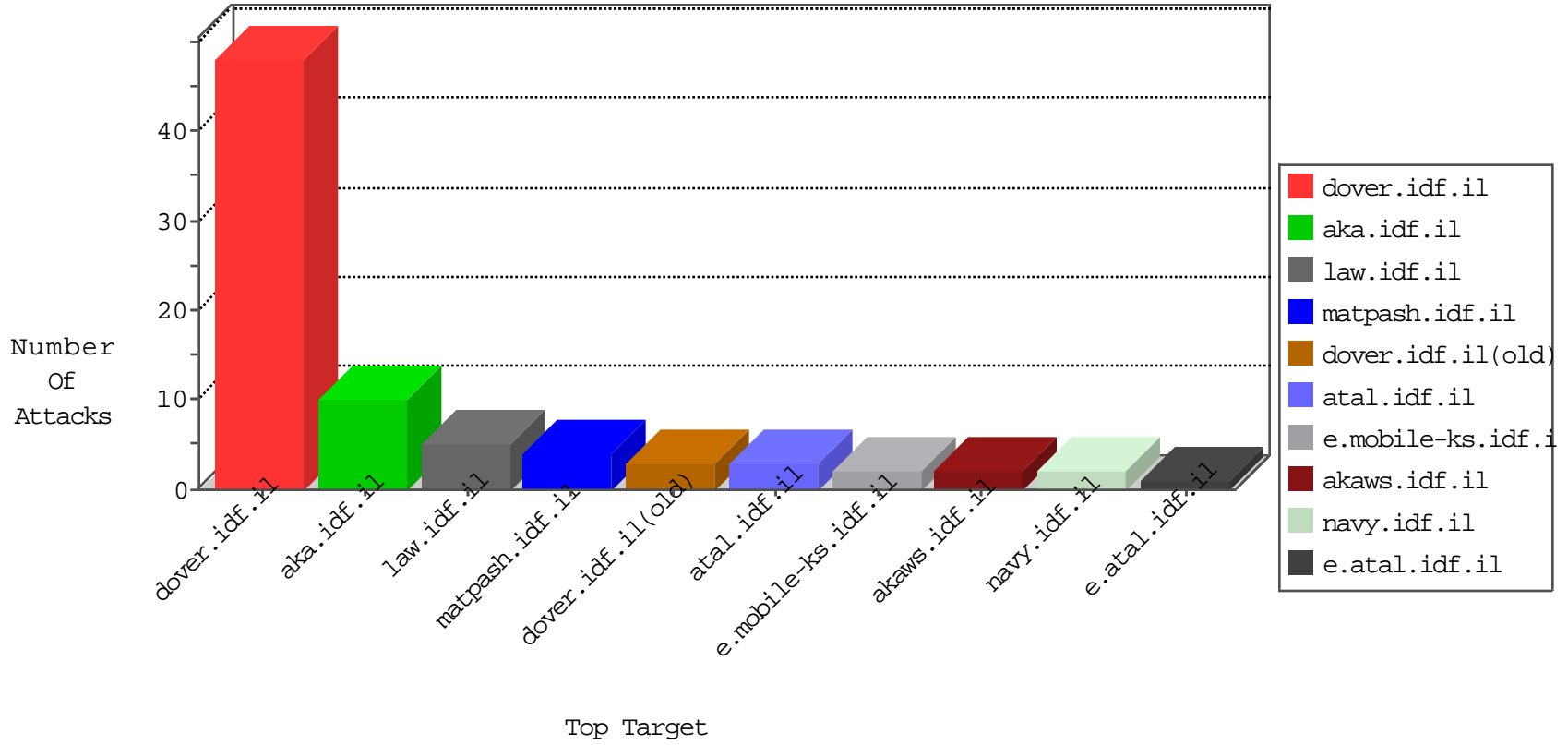


IDF Under Attack

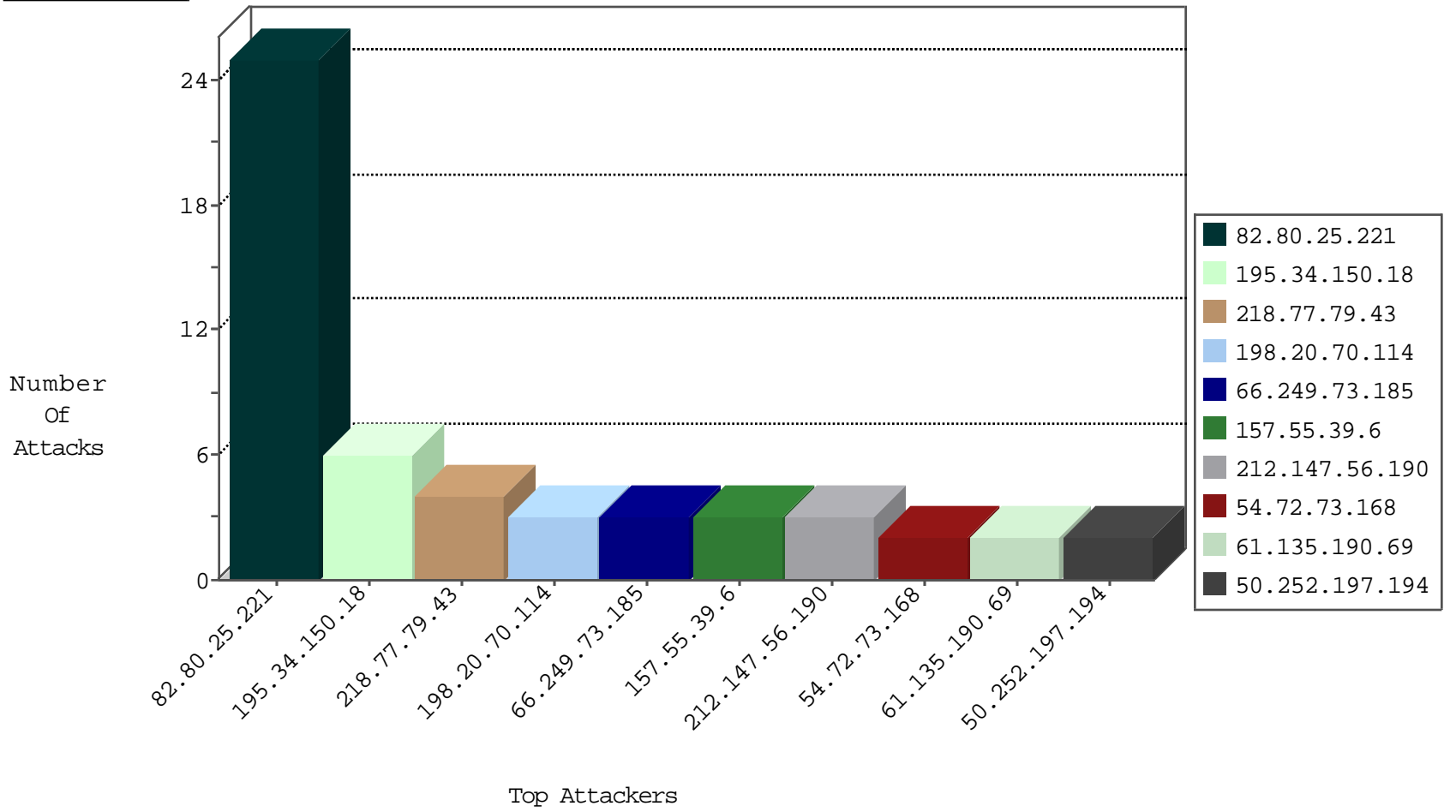
04-25-2015-09:03:10



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
52.74.49.82	United States	147.237.76.30	himush.idf.il	Invalid I4 Header Length	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
85.64.96.251	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.20.70.114	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
89.164.198.59	Croatia	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
198.20.69.98	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.57	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.201	e.atal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.198	e.yochalan.idf.il	DVRep_B-N_60_100	Block	1

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
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.78.197	United States	147.237.77.176	matpash.idf.il	ET SCAN NMAP -sA (2)	2
218.77.79.43	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
128.199.165.82	Singapore	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
61.240.144.66	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
50.252.197.194	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
212.147.56.190	Switzerland	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
182.254.226.90	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.67	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
50.252.197.194	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 3072	1
218.77.79.43	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
61.135.190.69	China	147.237.0.35	akaws.idf.il		drop	drop	1
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
173.252.74.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
173.252.74.113	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

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
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/mobile/	Block	1
66.249.69.86	Israel	147.237.77.226	www.charatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unknown Parameter 55bffe68 in www.aka.idf.il/main/home/default.aspx	None	1
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	1
52.6.31.228	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-6267-he/	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	1
157.55.39.39	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
61.135.190.69	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
104.32.162.117		147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11677en/dover.aspx	Block	1
46.117.162.166	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.62	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
66.249.69.36	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
46.121.80.11	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakchal.aspx	Block	1
157.55.39.179	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/news/www.israelbar.org.il	Block	1
66.249.75.68	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
66.249.69.76	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/english/main.asp	Block	1
52.6.31.228	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 52.6.31.228	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/announcements/2001/november/19.stm	Block	1