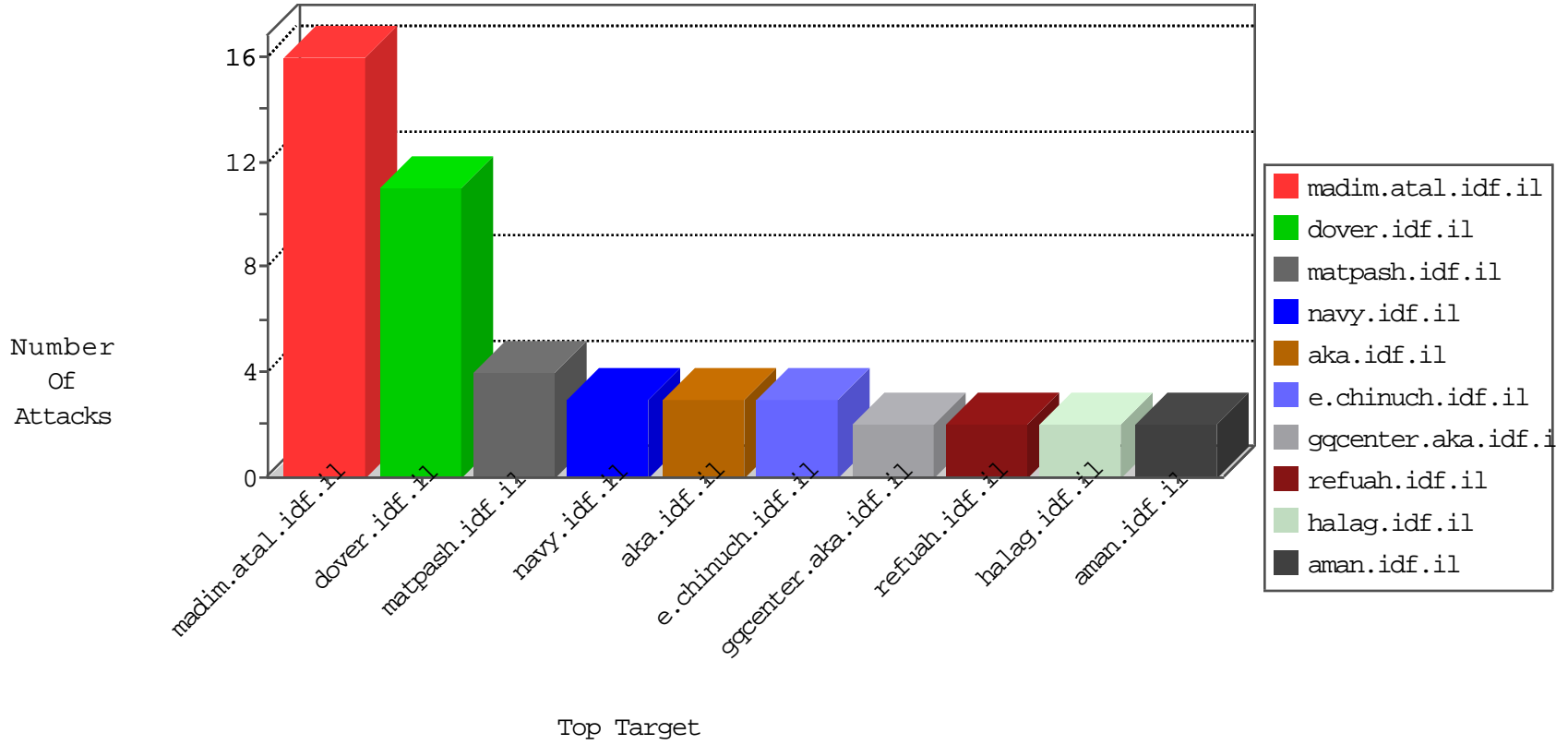


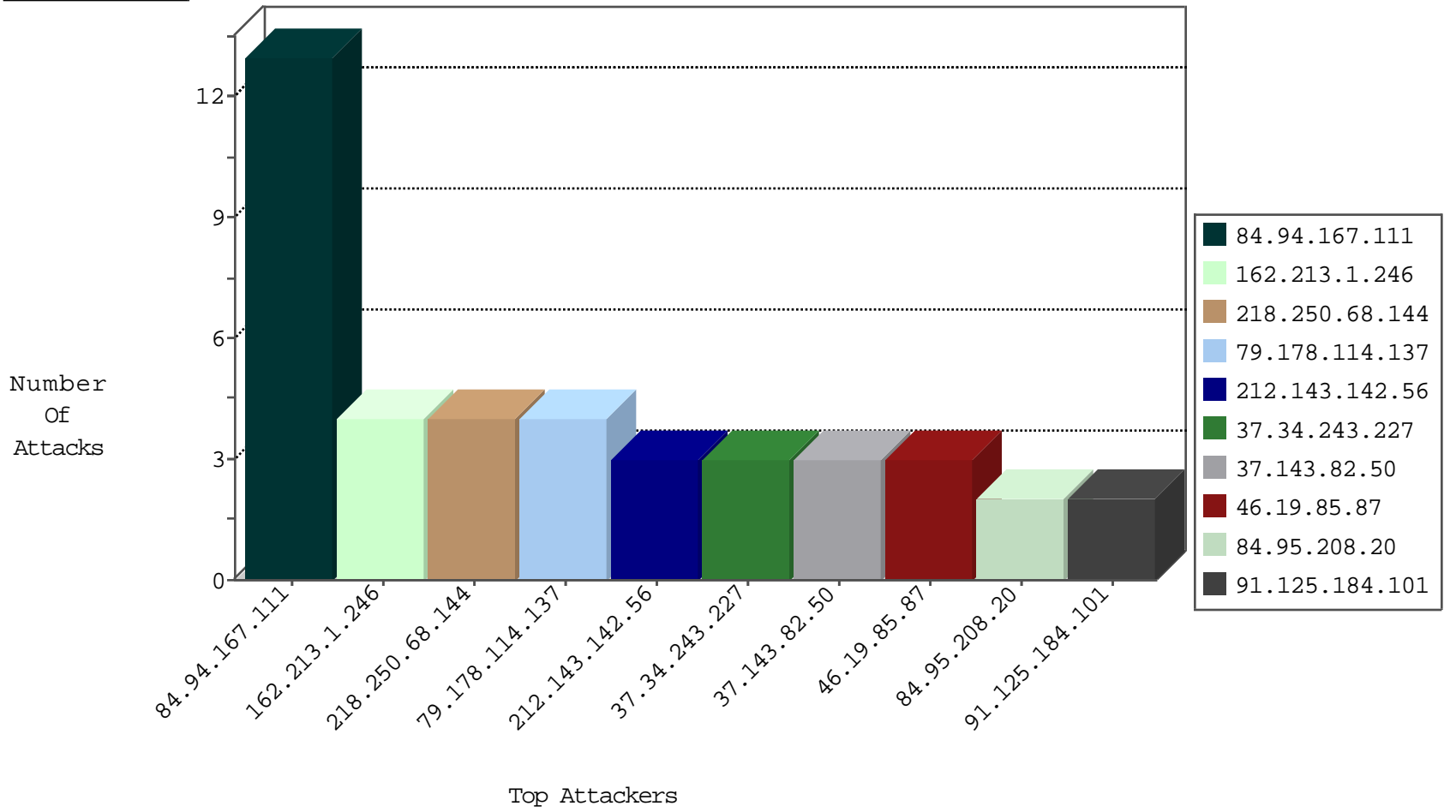
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
206.40.102.223	United States	147.237.76.86	navy.idf.il	Black List	drop	1
63.135.128.2	United States	147.237.76.86	navy.idf.il	Black List	drop	1
66.240.219.146	United States	147.237.76.148	ggcenter.aka.idf.il	Black List	drop	1
117.141.120.79	China	147.237.76.148	ggcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.65.73	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
182.108.37.210	China	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	4
218.250.68.144	147.237.8.14	Hong Kong	e.orchot.idf.il	ET SCAN Potential SSH Scan	2
46.228.207.18	147.237.76.197	Germany	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.143.82.50	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -f -sS	1
37.34.243.227	147.237.8.46	Kuwait	e.chinuch.idf.il	ET SCAN NMAP -sS window 2048	1
37.34.243.227	147.237.8.46	Kuwait	e.chinuch.idf.il	ET SCAN NMAP -f -sS	1
218.250.68.144	147.237.8.24	Hong Kong	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
207.191.195.138	147.237.76.30	United States	himush.idf.il	GPL SCAN PING CyberKit 2.2 Windows	1
91.125.184.101	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	1
66.249.79.169	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
37.143.82.50	147.237.77.234	Netherlands	halag.idf.il	ET SCAN NMAP -sS window 2048	1
37.143.82.50	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 4096	1
37.34.243.227	147.237.8.46	Kuwait	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
218.250.68.144	147.237.8.50	Hong Kong	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.125.184.101	147.237.77.176	United Kingdom	matpash.idf.il	Tehila - Perl LWP with fake user agent	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.69.113	Israel	147.237.0.33	idf.il	drop		drop	1
176.13.245.227	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.94.167.111	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	13
46.19.85.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.114.137	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
157.55.39.12	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-he	Block	1
77.127.37.129	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
180.76.15.134	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
79.178.114.137	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
62.203.33.33	Switzerland	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.178.114.137	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/wp-login.php	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.77	Block	1
79.178.114.137	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
99.234.250.119	Canada	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.127.37.129	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1