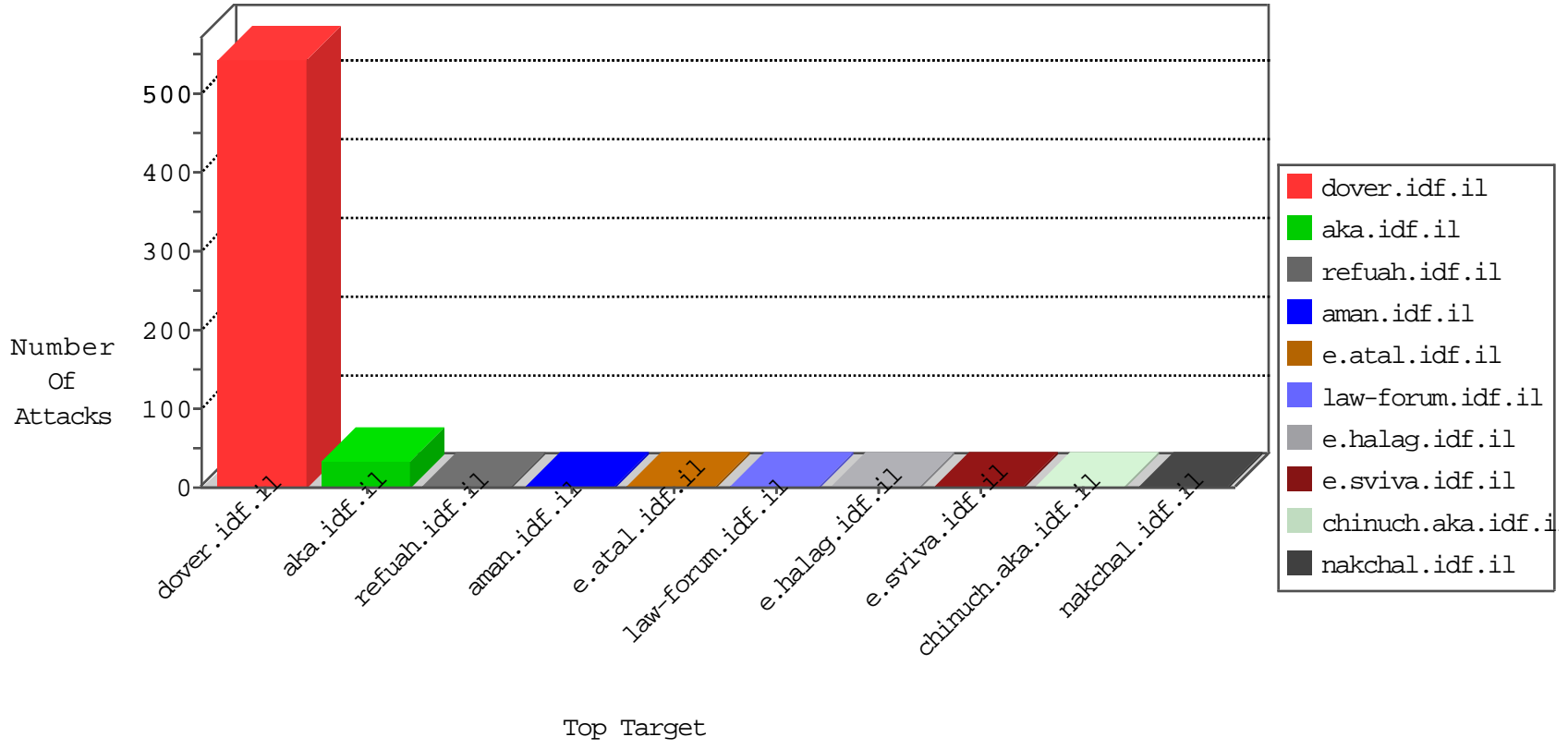


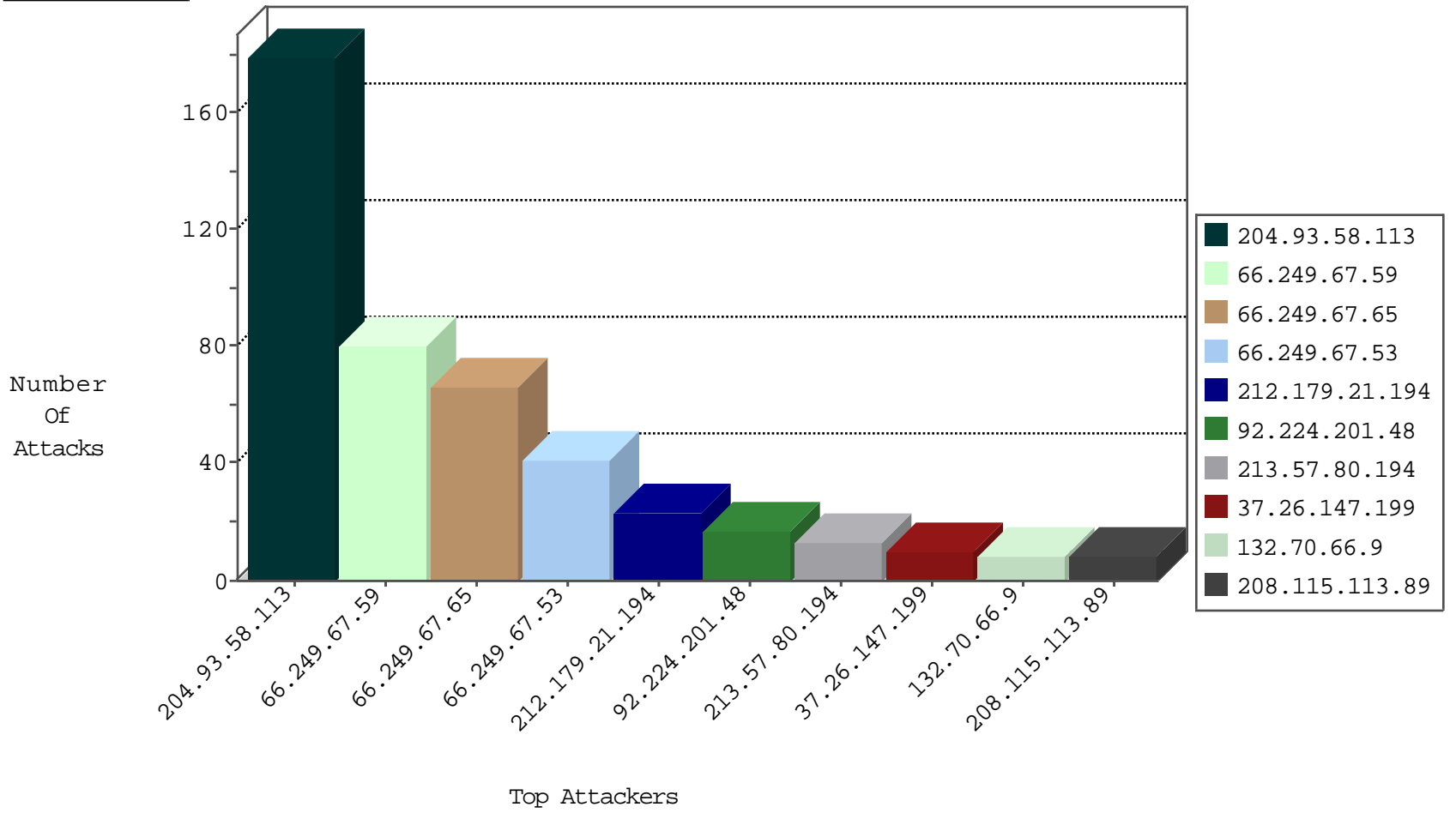
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.58.113	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	234860
66.249.67.59	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	152180
66.249.67.65	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	123243
66.249.67.53	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	65309
92.224.201.48	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	37860
141.0.15.225	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	18218
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	13894
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9754
207.241.237.209	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8089
75.43.18.202	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7284
178.6.236.110	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6960
66.249.67.77	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6627
65.19.138.34	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6522
198.58.102.156	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6468
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	23
37.26.147.199	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	10
132.70.66.9	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
213.57.80.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
149.88.185.178	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
208.115.113.89	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
92.224.201.48	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
37.26.147.247	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	6
213.57.80.194	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
195.147.232.147	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.13.6.59	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.235.170	Israel	147.237.76.42	refuah.idf.il	Invalid TCP Flags	drop	3
176.13.15.241	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
176.12.151.69	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
37.26.149.184	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.85.182	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
37.26.147.140	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
46.19.86.246	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
2.54.181.142	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
2.54.9.134	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
93.172.152.233	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
2.54.37.139	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
2.54.9.134	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
198.58.96.215	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
37.24.147.73	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
176.12.142.85	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
2.54.43.119	Israel	147.237.72.156	aman.idf.il	network flood IPv4 TCP-SYN	drop	1
46.19.86.118	Israel	147.237.72.166	aka.idf.il	network flood IPv4 TCP-SYN	drop	1
188.165.15.126	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.85.102	Israel	147.237.72.156	aman.idf.il	network flood IPv4 TCP-SYN	drop	1
66.249.67.83	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
5.28.170.44	Israel	147.237.77.216	dover.idf.il	network flood IPv4 TCP-SYN	drop	1

10-25-2015-13:04:05 to 10-25-2015-14:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
104.43.200.179	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
77.236.96.52	147.237.76.201	Germany	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.126	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
104.43.200.179	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
77.236.96.52	147.237.76.147	Germany	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
------------------	------------------	----------------	------	-----------	---------	---------------	-------

10-25-2015-13:04:05 to 10-25-2015-14:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

10-25-2015-13:04:05 to 10-25-2015-14:04:05