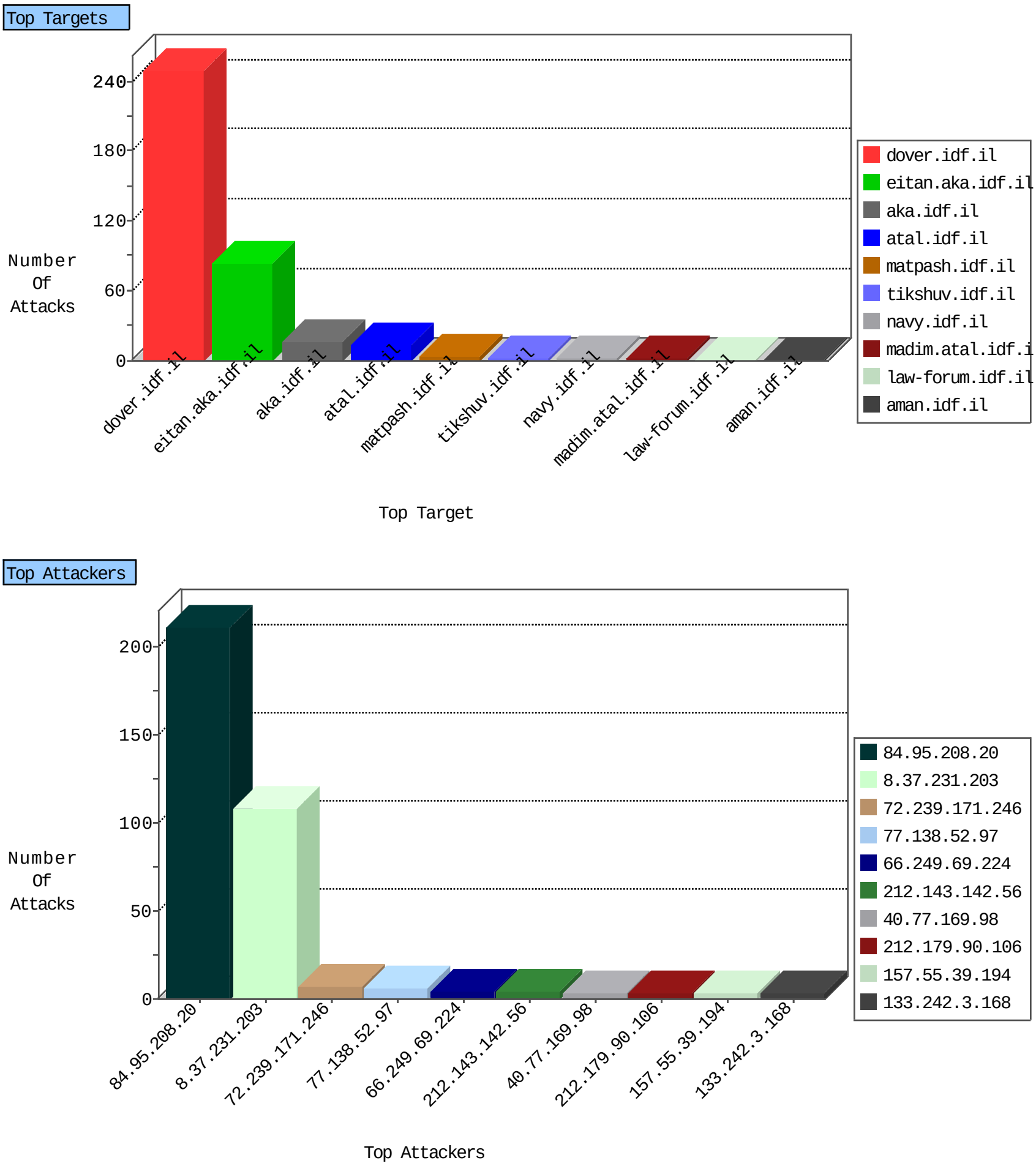
08-24-2016-03:04:02 to 08-24-2016-04:04:02

IDF Under Attack Daily Report



08-24-2016-03:04:02 to 08-24-2016-04:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
157.55.39.194	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
8.37.231.203	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
46.101.182.173	Germany	147.237.76.196	e.sviva.idf.il	Black List	drop	1
149.56.200.203	United States	147.237.76.86	navy.idf.il	Black List	drop	1

08-24-2016-03:04:02 to 08-24-2016-04:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-24-2016-03:04:02 to 08-24-2016-04:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
59.67.64.13	147.237.0.19	China	madim.atal.idf.il	GPL SCAN nmap TCP	2
202.155.58.28	147.237.76.199	Indonesia	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
186.170.230.221	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
133.242.3.168	147.237.77.235	Japan	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.39	Netherlands	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
66.240.213.93	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
202.155.58.28	147.237.77.19	Indonesia	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.208.193	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
186.170.212.135	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
133.242.3.168	147.237.76.177	Japan	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.117	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
66.240.213.93	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1

08-24-2016-03:04:02 to 08-24-2016-04:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.231.203	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	67
8.37.231.203	United States	147.237.77.216	dover.idf.il	drop		drop	38
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.37	China	147.237.0.200	m4u.idf.il	drop		drop	1
89.151.191.4	Russian Federation	147.237.76.34	yohalan.idf.il	drop		drop	1
133.242.3.168	Japan	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1

08-24-2016-03:04:02 to 08-24-2016-04:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	102
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.i	Multiple Unauthorized URL Access from 84.95.208.20	Block	84
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
72.239.171.246	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	7
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	6
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	4
93.172.218.33	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
79.180.41.143	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.119.127.129	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
220.202.123.178	China	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
157.55.39.132	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
79.180.44.64	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	1
46.119.127.129	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.119.127.129	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
71.6.135.131	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
178.154.149.7	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/hebrew/asp/default.asp	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
42.200.34.83	Hong Kong	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
192.243.55.137	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
66.249.75.64	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19667-he/idfgdover.aspx	Block	1
79.180.41.143	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 79.180.41.143 (Open Mode)	None	1
42.200.34.83	Hong Kong	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
219.75.81.197	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1

08-24-2016-03:04:02 to 08-24-2016-04:04:02