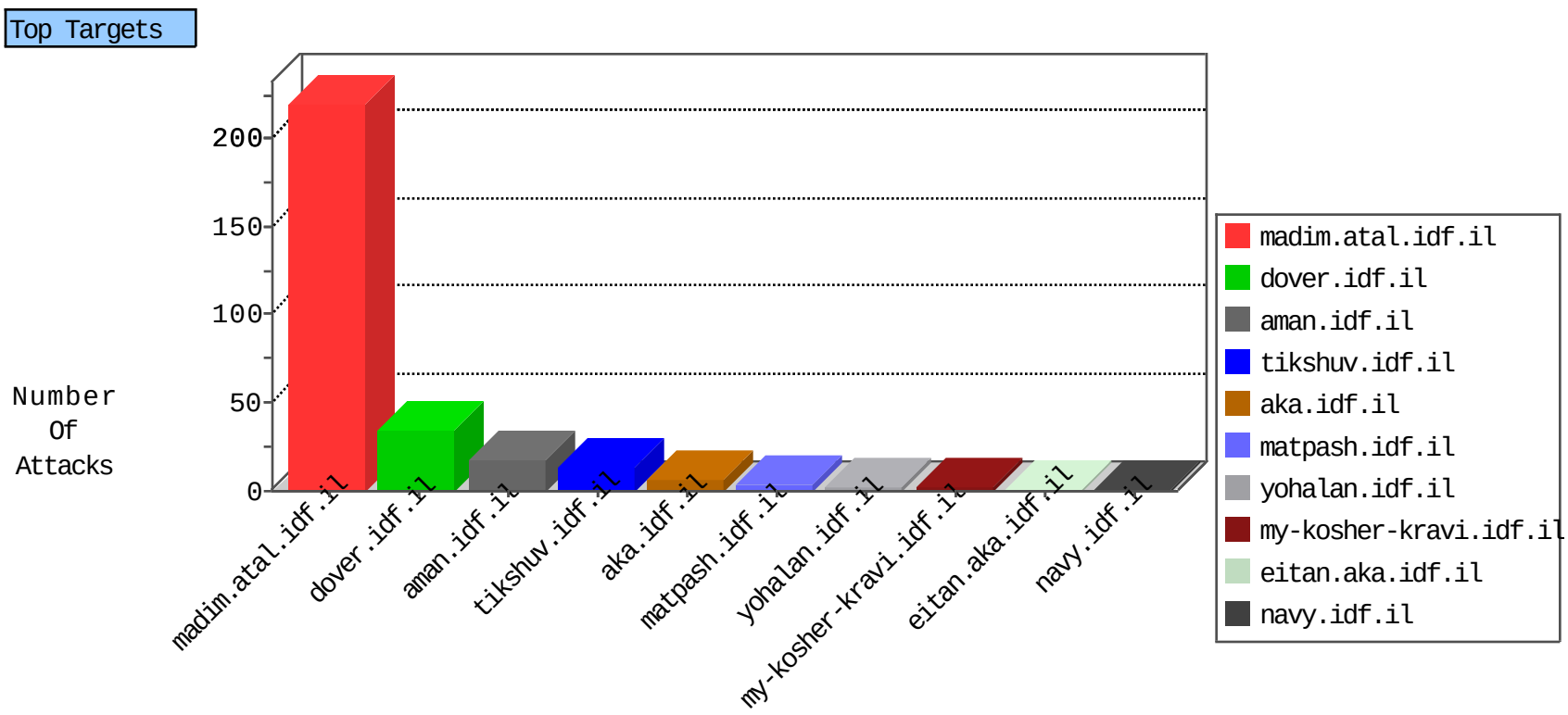
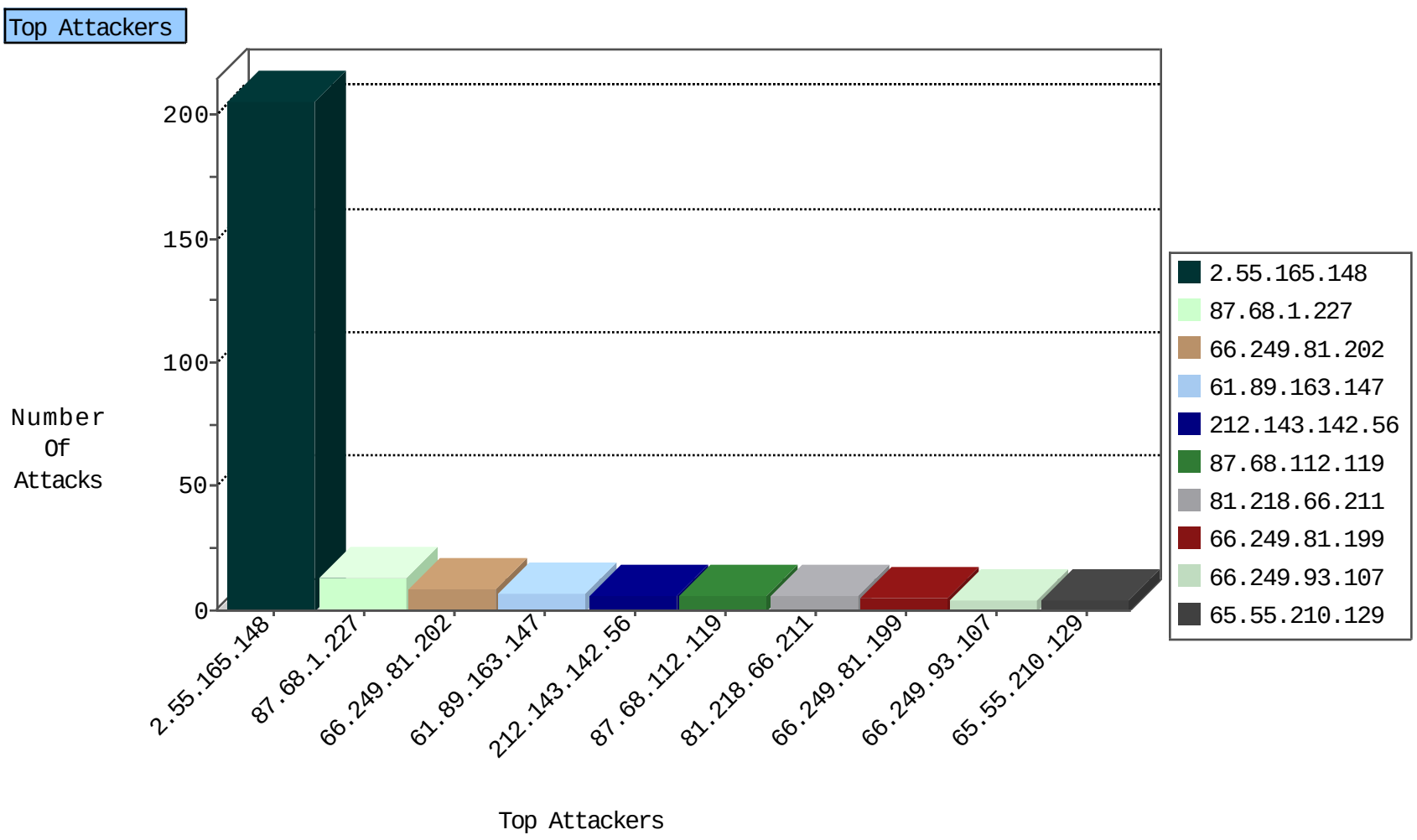
08-20-2016-17:04:02 to 08-20-2016-18:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-20-2016-17:04:02 to 08-20-2016-18:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	3
93.174.95.106	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
123.151.42.61	China	147.237.76.34	yohalan.idf.il	JLM_Purple_Con_Limit_Udp	drop	1
123.151.42.61	China	147.237.76.34	yohalan.idf.il	JLM_Under_Attack_Con_Udp	drop	1

08-20-2016-17:04:02 to 08-20-2016-18:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.89.163.147	Japan	147.237.77.216	dover.idf.il	C1000064: HTTP: Access to - admin.asp	Permit	5

08-20-2016-17:04:02 to 08-20-2016-18:04:02

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
198.20.69.98	147.237.77.19	United States	law-forum.idf.il	ET DROP Dshield Block Listed Source	1
14.148.239.198	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

08-20-2016-17:04:02 to 08-20-2016-18:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.68.1.227	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	13
66.249.81.202	Europe	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	9
81.218.66.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.81.199	Europe	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
89.139.206.132	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	3
66.249.93.107	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
66.249.93.107	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
66.249.81.199	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	1
66.249.93.107	Israel	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1

08-20-2016-17:04:02 to 08-20-2016-18:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.165.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	206
87.68.112.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
65.55.210.129	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.116.43.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
81.218.127.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
157.55.2.166	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
199.30.25.6	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.139.77.217	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/shalishut/site/default.aspx	Block	2
66.249.66.242	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
79.176.104.111	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.64	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
79.180.125.136	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.102.9.8	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
176.13.8.209	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector/	Block	1
66.249.69.126	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
46.117.24.172	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyius/home/default.aspx	Block	1
66.102.9.85	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
197.40.142.212	Egypt	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 197.40.142.212 (Open Mode)	None	1
77.138.220.176	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
61.89.163.147	Japan	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
84.108.15.250	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/homepage/homepage.aspx	Block	1
66.249.64.193	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1321-he/אגף הטכנולוגיה והלוגיסטיקה.aspx	Block	1
61.89.163.147	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/admin/	Block	1

08-20-2016-17:04:02 to 08-20-2016-18:04:02