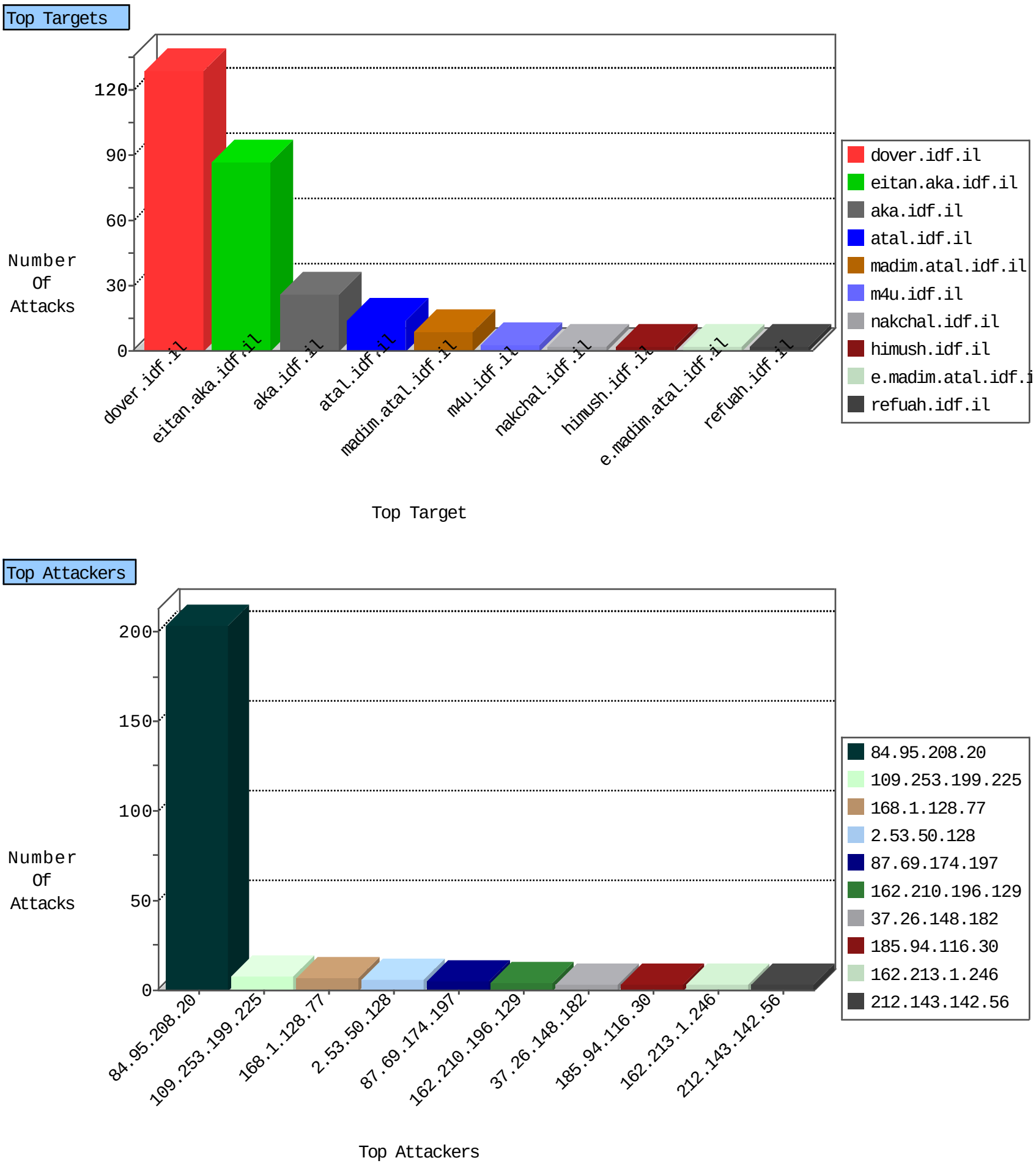
08-21-2016-03:04:07 to 08-21-2016-04:04:07

IDF Under Attack
Daily Report



08-21-2016-03:04:07 to 08-21-2016-04:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
168.1.128.77	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	1
103.29.5.8	Indonesia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
168.1.128.77	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
66.240.236.119	United States	147.237.76.31	nakchal.idf.il	Black List	drop	1
168.1.128.77	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
119.110.80.21	Indonesia	147.237.0.34	tikshuv.idf.il	Invalid TCP Flags	drop	1
212.159.128.34	United Kingdom	147.237.76.30	himush.idf.il	Black List	drop	1
168.1.128.77	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
168.1.128.77	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
119.110.80.21	Indonesia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
212.159.128.34	United Kingdom	147.237.76.31	nakchal.idf.il	Black List	drop	1
168.1.128.77	United States	147.237.76.176	test.ncore.idf.il	Black List	drop	1
103.29.5.8	Indonesia	147.237.0.34	tikshuv.idf.il	Invalid TCP Flags	drop	1
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Black List	drop	1
168.1.128.77	United States	147.237.76.30	himush.idf.il	Black List	drop	1

08-21-2016-03:04:07 to 08-21-2016-04:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.94.116.30	United Kingdom	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	3
149.202.54.50	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.129	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.129	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
164.132.161.89	Italy	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.81	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-21-2016-03:04:07 to 08-21-2016-04:04:07

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	3
91.125.184.101	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1
211.23.156.152	147.237.0.200	Taiwan	m4u.idf.il	ET SCAN Potential SSH Scan	1
177.207.21.186	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
173.208.249.35	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
118.243.220.141	147.237.0.17	Japan	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
91.125.184.101	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	1
211.23.156.152	147.237.76.42	Taiwan	refuah.idf.il	ET SCAN Potential SSH Scan	1
193.201.225.138	147.237.77.19	Ukraine	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
173.208.249.35	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
103.207.38.14	147.237.77.234	Vietnam	halag.idf.il	ET SCAN NMAP -sS window 1024	1

08-21-2016-03:04:07 to 08-21-2016-04:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.199.225	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
162.243.253.50	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.9.62.130	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
109.64.104.32	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.149	United States	147.237.0.200	m4u.idf.il	drop		drop	1
107.0.218.53	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
176.13.11.109	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
185.125.4.222	Poland	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
65.210.36.98	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.148	United States	147.237.0.200	m4u.idf.il	drop		drop	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-21-2016-03:04:07 to 08-21-2016-04:04:07

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	100
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	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
2.53.50.128	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	6
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	6
87.69.174.197	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.174.197	Block	4
37.26.148.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
204.79.180.96	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
66.249.83.242	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
204.79.180.110	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
5.102.242.63	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
87.69.174.197	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/giyus	Block	1
77.138.207.46	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
204.79.180.215	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
121.42.54.54	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
66.102.6.188	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
121.42.54.54	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
220.255.219.58	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1

08-21-2016-03:04:07 to 08-21-2016-04:04:07