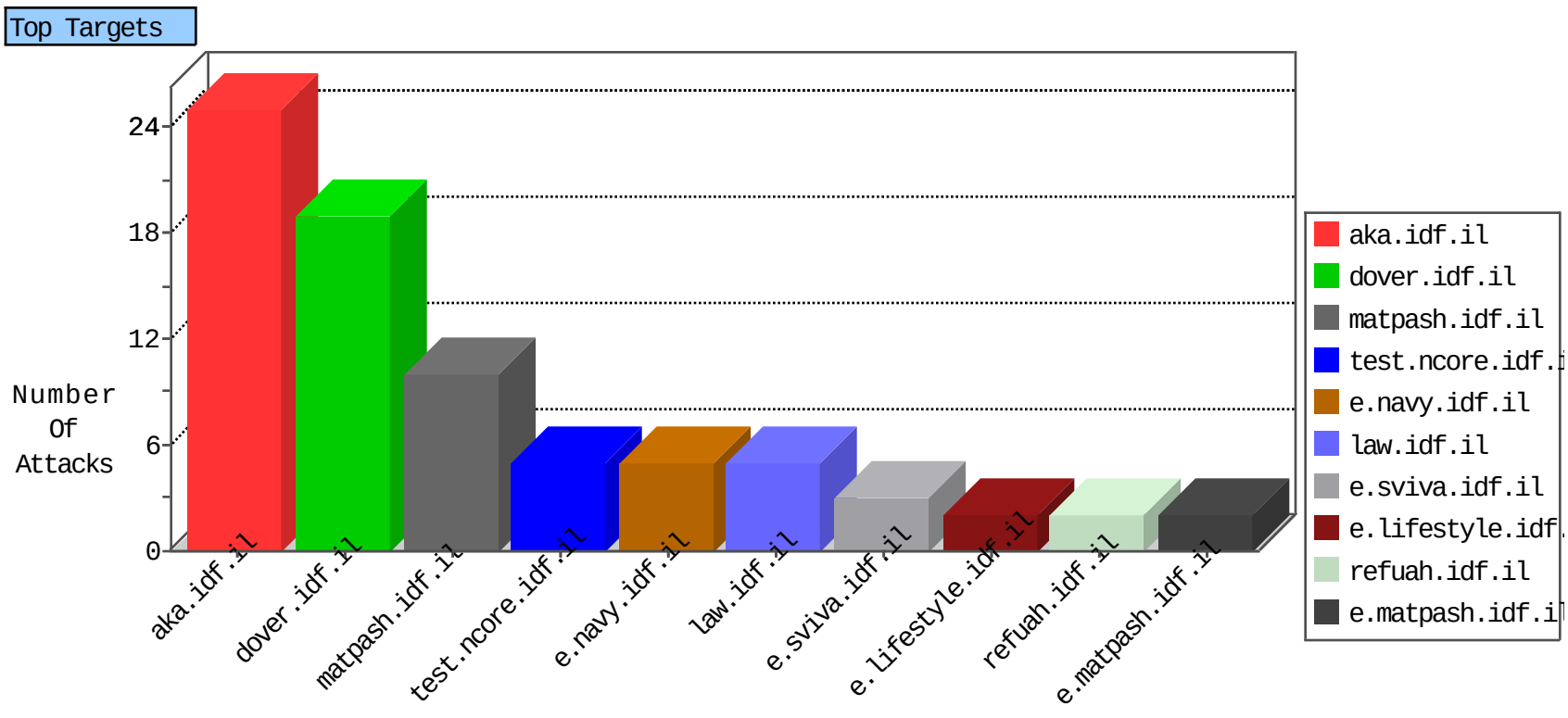
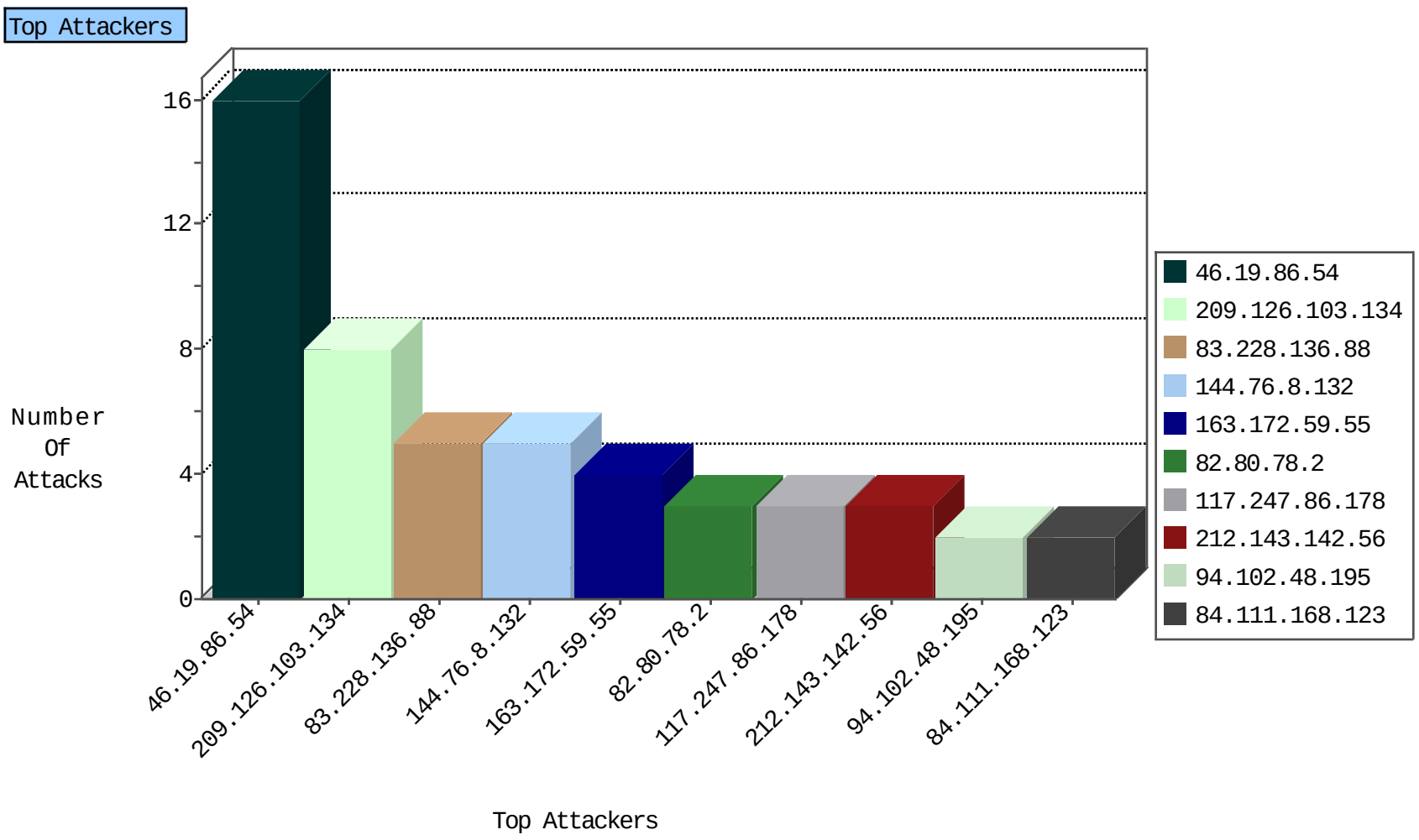
08-18-2016-04:04:07 to 08-18-2016-05:04:07

IDF Under Attack
Daily Report





08-18-2016-04:04:07 to 08-18-2016-05:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
209.126.103.134	United States	147.237.76.176	test.ncore.idf.il	Black List	drop	5
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	3
209.126.103.134	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	3
89.248.171.2	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1
89.248.171.2	Netherlands	147.237.76.200	eitan.aka.idf.il	Black List	drop	1

08-18-2016-04:04:07 to 08-18-2016-05:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.8.132	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
94.154.239.69	Ukraine	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
144.76.8.132	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
151.80.31.171	France	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

08-18-2016-04:04:07 to 08-18-2016-05:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.201.236.50	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
200.195.135.82	147.237.76.39	Brazil	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
66.249.65.151	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
187.13.107.245	147.237.77.216	Brazil	dover.idf.il	ET SCAN NMAP -sS window 4096	1
180.97.75.130	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
173.208.249.37	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.59.55	147.237.77.74	United Kingdom	law.idf.il	ET SCAN Potential SSH Scan	1
163.172.59.55	147.237.76.199	United Kingdom	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
113.108.10.31	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.195	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
82.20.219.5	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
200.195.135.82	147.237.76.39	Brazil	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
180.97.75.130	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
173.208.249.37	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
163.172.59.55	147.237.77.121	United Kingdom	e.navy.idf.il	ET SCAN Potential SSH Scan	1
163.172.59.55	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN Potential SSH Scan	1
117.247.86.178	147.237.77.121	India	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1

08-18-2016-04:04:07 to 08-18-2016-05:04:07

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	3
83.228.136.88	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.147.119.66	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
213.191.16.248	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
117.247.86.178	India	147.237.77.121	e.navy.idf.il	drop	First packet isn't SYN	drop	2
176.195.98.124	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
216.218.206.82	United States	147.237.0.200	m4u.idf.il	drop		drop	1

08-18-2016-04:04:07 to 08-18-2016-05:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.54	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.19.86.54	Block	13
46.19.86.54	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	2
136.243.16.208	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
66.249.66.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19891-he/idfgdover.aspx	Block	1
87.70.247.126	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
75.77.34.67	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
89.248.172.16	Netherlands	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
157.55.39.164	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/general.aspx	Block	1
84.111.168.123	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
120.27.115.58	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for aka.idf.il/main/home/default.aspx	Block	1
46.19.86.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
192.243.55.136	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcdhphdmltxdk4mc5kb2m=&infocenteritem=true	Block	1
84.111.168.123	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
136.243.16.208	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 136.243.16.208	Block	1
66.249.66.169	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/894-he	Block	1
207.46.13.145	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
87.70.247.126	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1

08-18-2016-04:04:07 to 08-18-2016-05:04:07