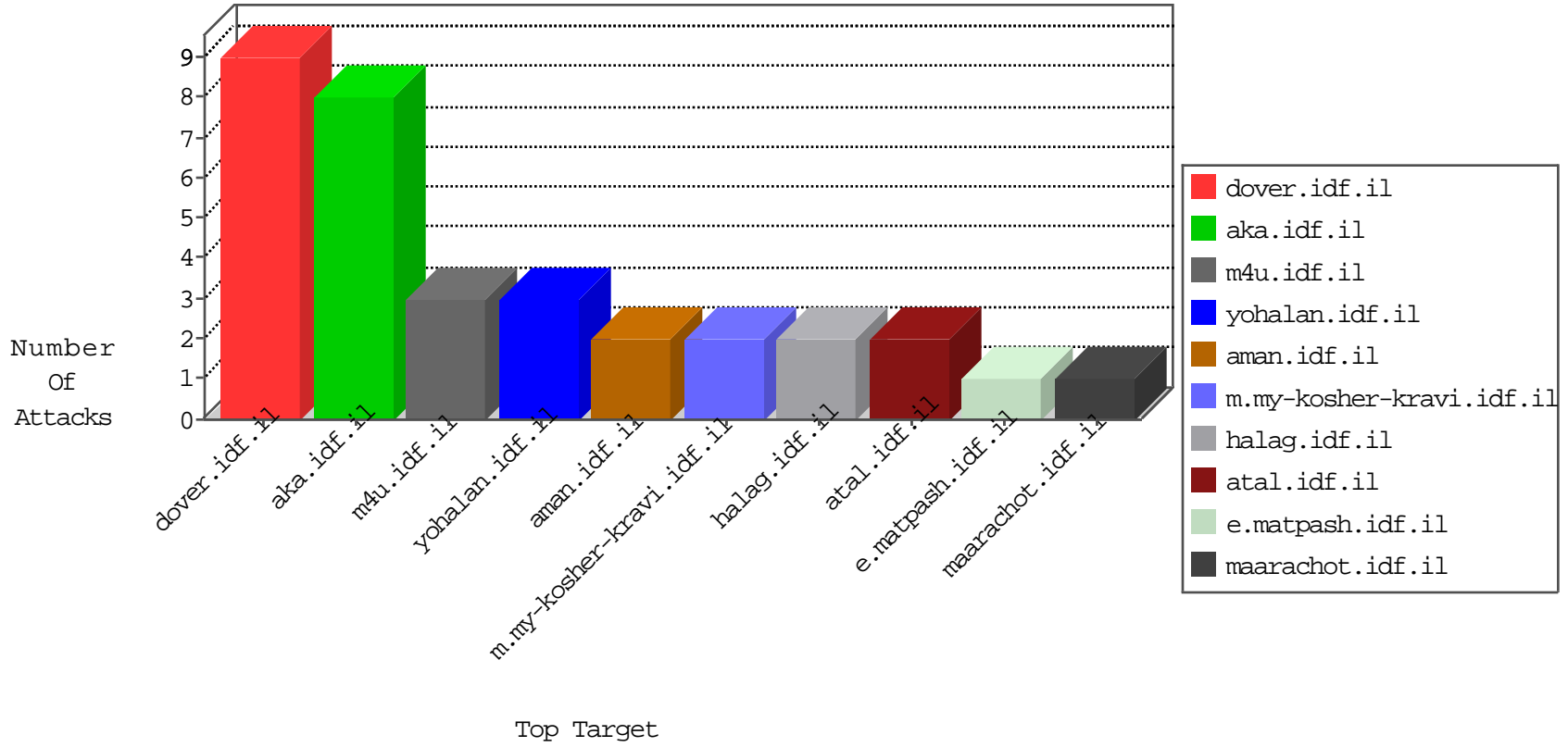


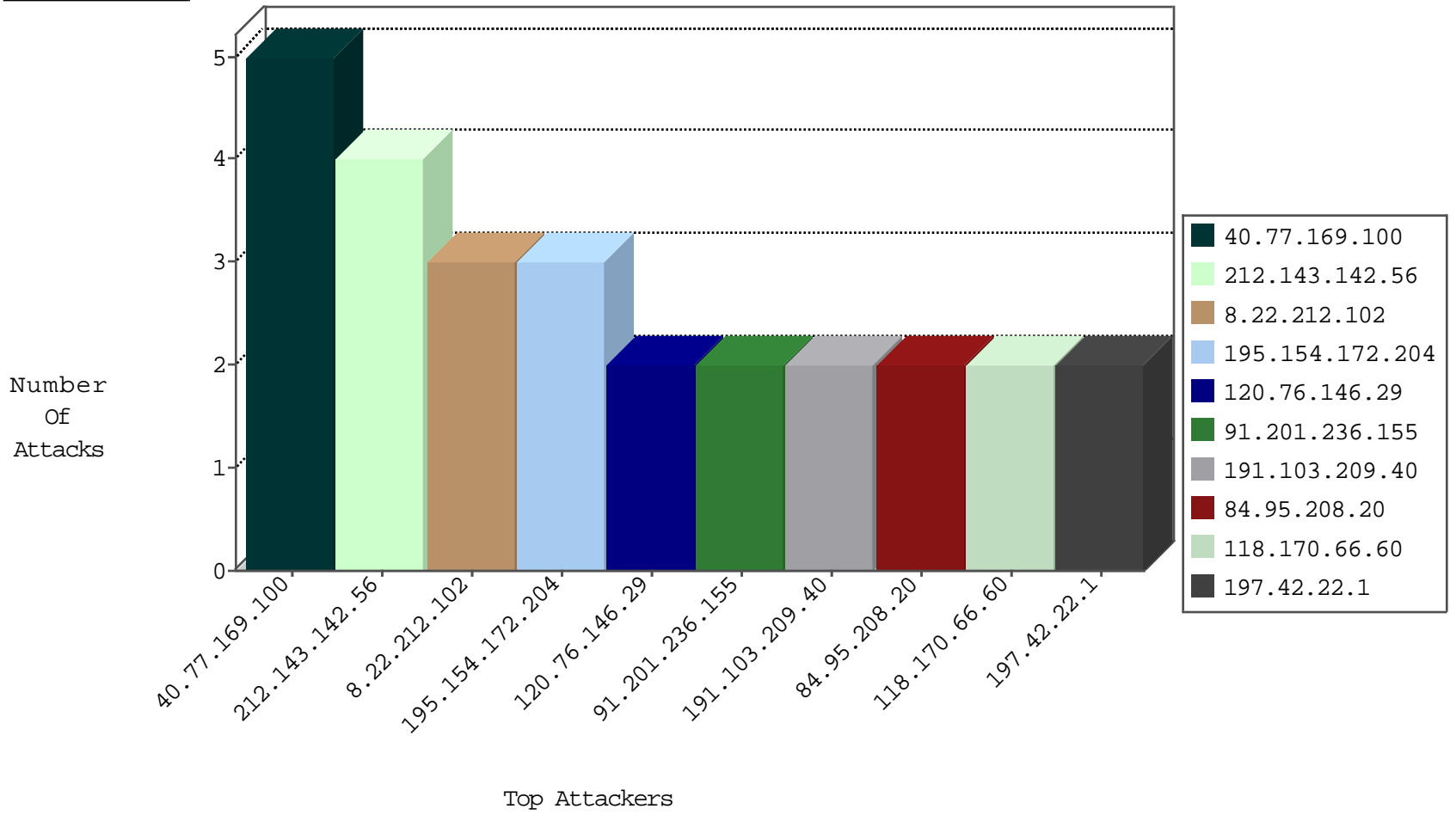
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.56.200.203	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.34	yohalan.idf.il	Black List	drop	1
195.154.172.204	France	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1
195.154.172.204	France	147.237.72.166	aka.idf.il	JLM_Purple_Con_Limit_Http	drop	1
64.74.97.49	United States	147.237.76.176	test.ncore.idf.il	Black List	drop	1
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1

08-24-2016-04:04:01 to 08-24-2016-05:04:01

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
8.22.212.102	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
8.22.212.102	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
220.132.101.33	147.237.8.24	Taiwan	e.lifestyle.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
178.220.169.35	147.237.77.178		e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
128.199.70.132	147.237.77.227	Singapore	e.hamaz.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
118.170.66.60	147.237.72.14	Taiwan	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
85.104.101.65	147.237.76.31	Turkey	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
195.88.208.193	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
133.242.4.52	147.237.77.233	Japan	atal.idf.il	ET SCAN NMAP -sS window 1024	1
118.170.66.60	147.237.72.166	Taiwan	aka.idf.il	ET SCAN Potential SSH Scan	1
93.174.91.29	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
197.42.22.1	Egypt	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	2
89.151.191.4	Russian Federation	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
180.97.106.162	China	147.237.0.33	idf.il	drop		drop	1
185.125.4.222	Poland	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
195.154.172.204	France	147.237.76.34	yohalan.idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
191.103.209.40	Colombia	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1673	Block	1
98.169.61.8	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.76.39	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/apple-app-site-association	Block	1
120.76.146.29	China	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
73.250.57.135	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
120.76.146.29	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/wp-login.php	Block	1
66.249.64.21	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
66.249.64.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/key/aswd56425csa	Block	1