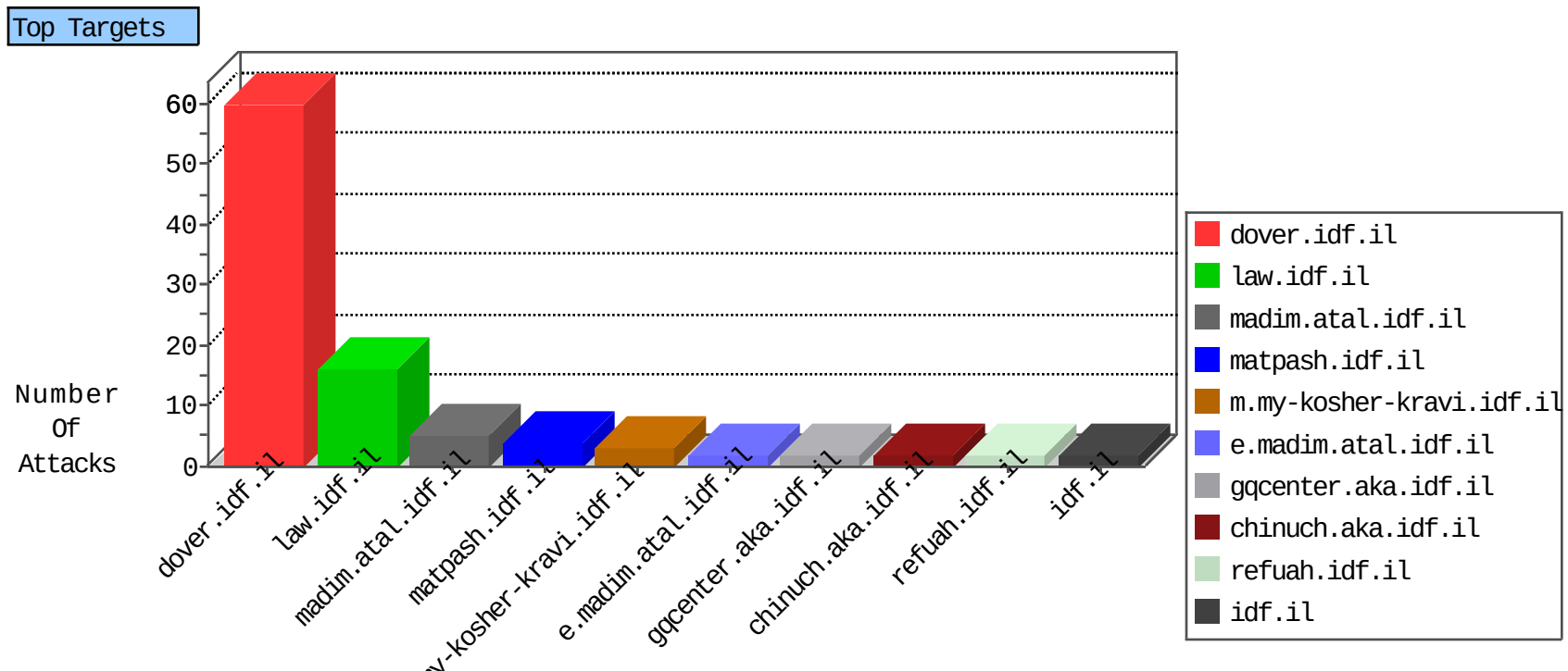
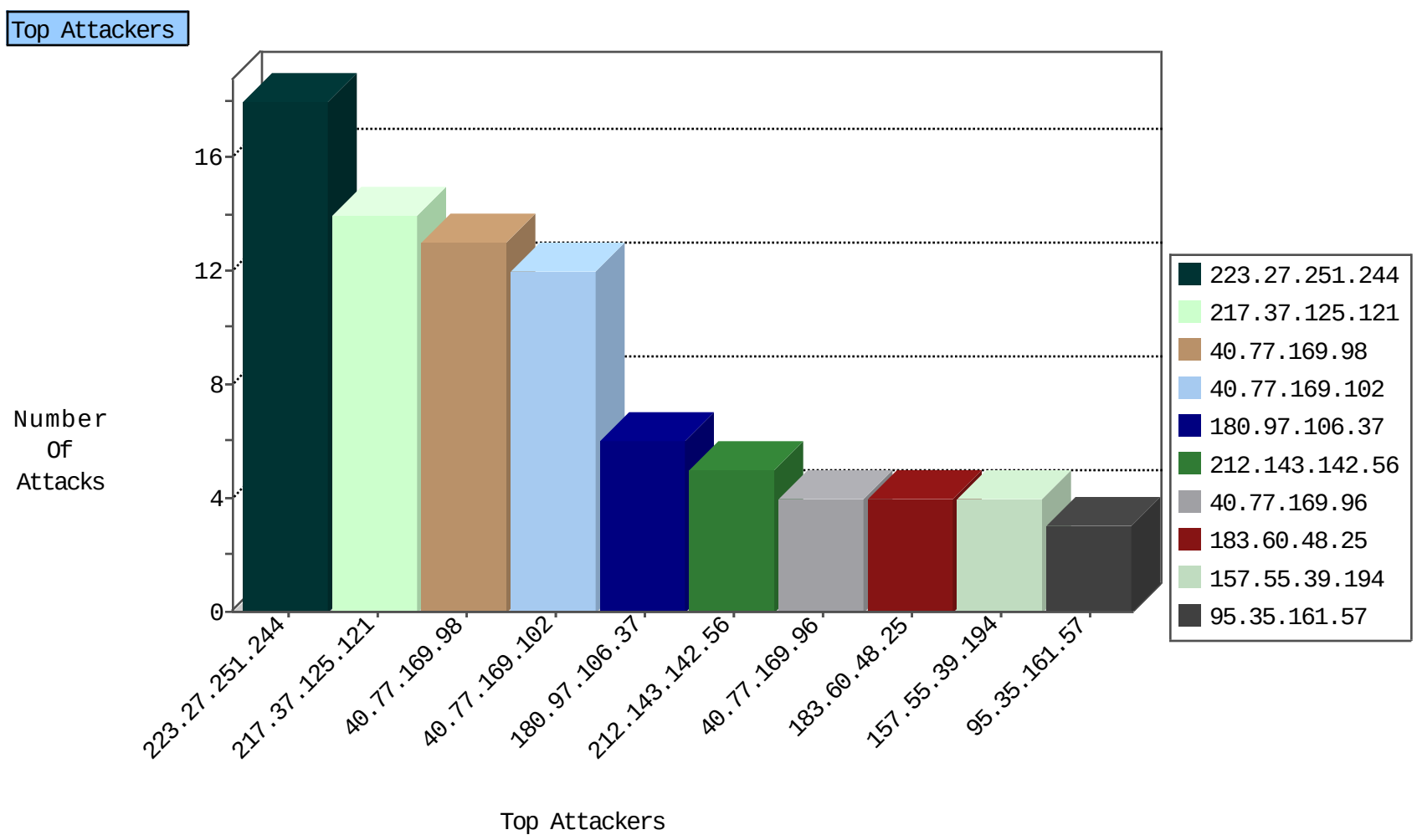
08-25-2016-04:04:00 to 08-25-2016-05:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-25-2016-04:04:00 to 08-25-2016-05:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
104.148.55.162	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
89.248.168.21	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Black List	drop	1
104.148.55.162	United States	147.237.76.30	himush.idf.il	Black List	drop	1
104.148.55.162	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
66.240.192.138	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

08-25-2016-04:04:00 to 08-25-2016-05:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.37.125.121	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
66.240.236.119	United States	147.237.76.202	e.halag.idf.i	13840: TLS: OpenSSL Heartbeat Packet	Block	1
52.39.51.60	United States	147.237.76.86	navy.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1

08-25-2016-04:04:00 to 08-25-2016-05:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
217.37.125.121	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	8
139.162.13.205	147.237.8.27	Singapore	e.madim.atal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
131.0.96.194	147.237.76.198	Brazil	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
201.238.202.219	147.237.8.46	Chile	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
180.97.75.130	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
177.159.146.152	147.237.77.216	Brazil	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
133.242.3.168	147.237.76.176	Japan	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
129.56.2.38	147.237.77.170	Nigeria	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
203.4.240.101	147.237.76.201	Australia	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
201.238.202.219	147.237.8.27	Chile	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
180.97.75.130	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1

08-25-2016-04:04:00 to 08-25-2016-05:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
223.27.251.244	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
40.77.169.102	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
185.120.125.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.80	United States	147.237.0.33	idf.il	drop		drop	1
61.136.195.22	China	147.237.0.33	idf.il	drop		drop	1
89.248.174.4	Netherlands	147.237.0.200	m4u.idf.il	drop		drop	1

08-25-2016-04:04:00 to 08-25-2016-05:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.35.161.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
157.55.39.194	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
82.166.240.204	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
157.55.39.194	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	2
180.97.106.37	China	147.237.76.39	mobile.meitav.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
66.249.75.68	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21147-he/idfgdover.aspx	Block	1
66.249.64.147	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
180.97.106.37	China	147.237.76.39	mobile.meitav.idf.il	Distributed NULL Character in Method	Block	1
180.97.106.37	China	147.237.77.74	law.idf.il	Multiple Illegal Byte Code Character in Method from 180.97.106.37	Block	1
180.97.106.37	China	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Method	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/langstyle.css	Block	1
180.97.106.37	China	147.237.77.74	law.idf.il	Multiple NULL Character in Method from 180.97.106.37	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
40.77.169.97	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
180.97.106.37	China	147.237.0.17	m.my-kosher-kravi.idf.il	NULL Character in Method	Block	1
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-ui.js	Block	1
157.55.39.37	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.169.101	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1

08-25-2016-04:04:00 to 08-25-2016-05:04:00