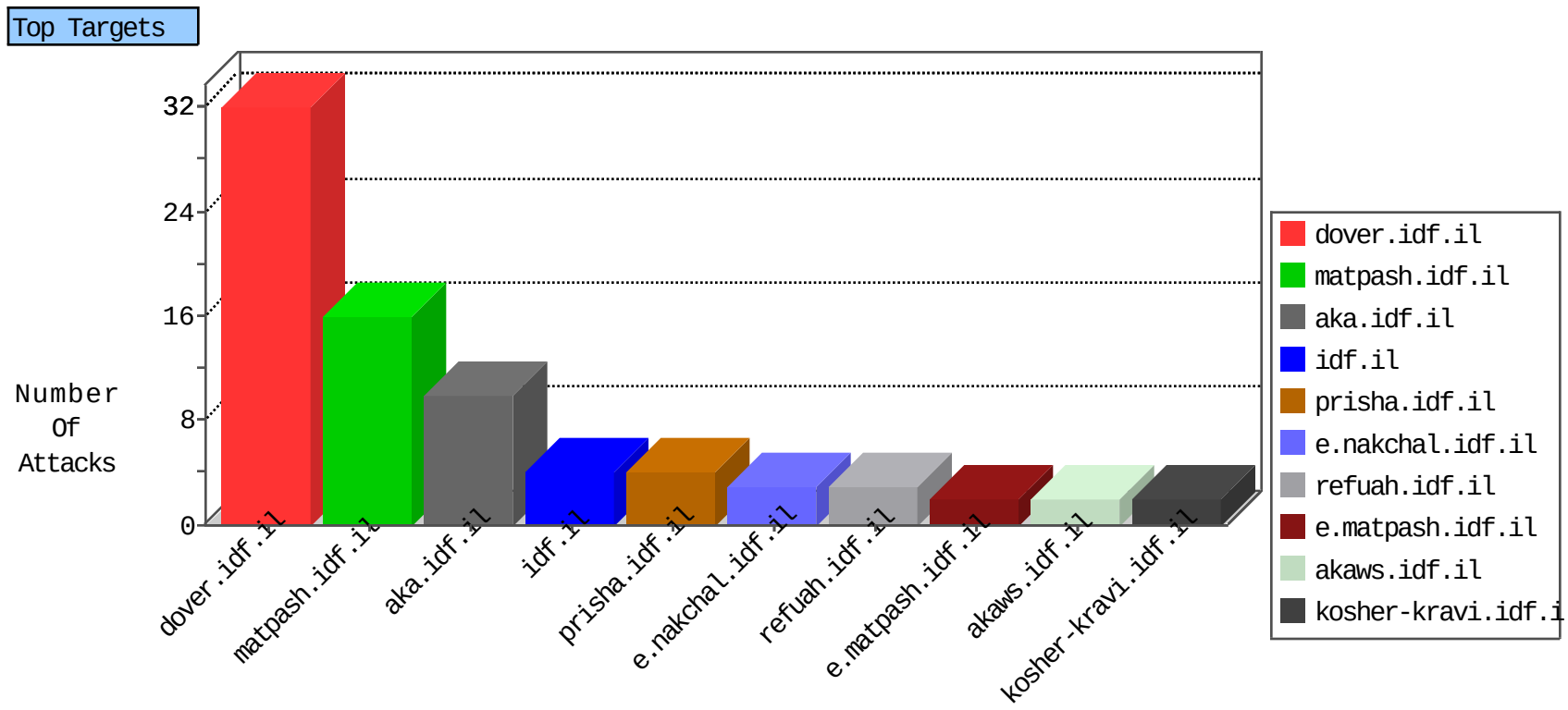
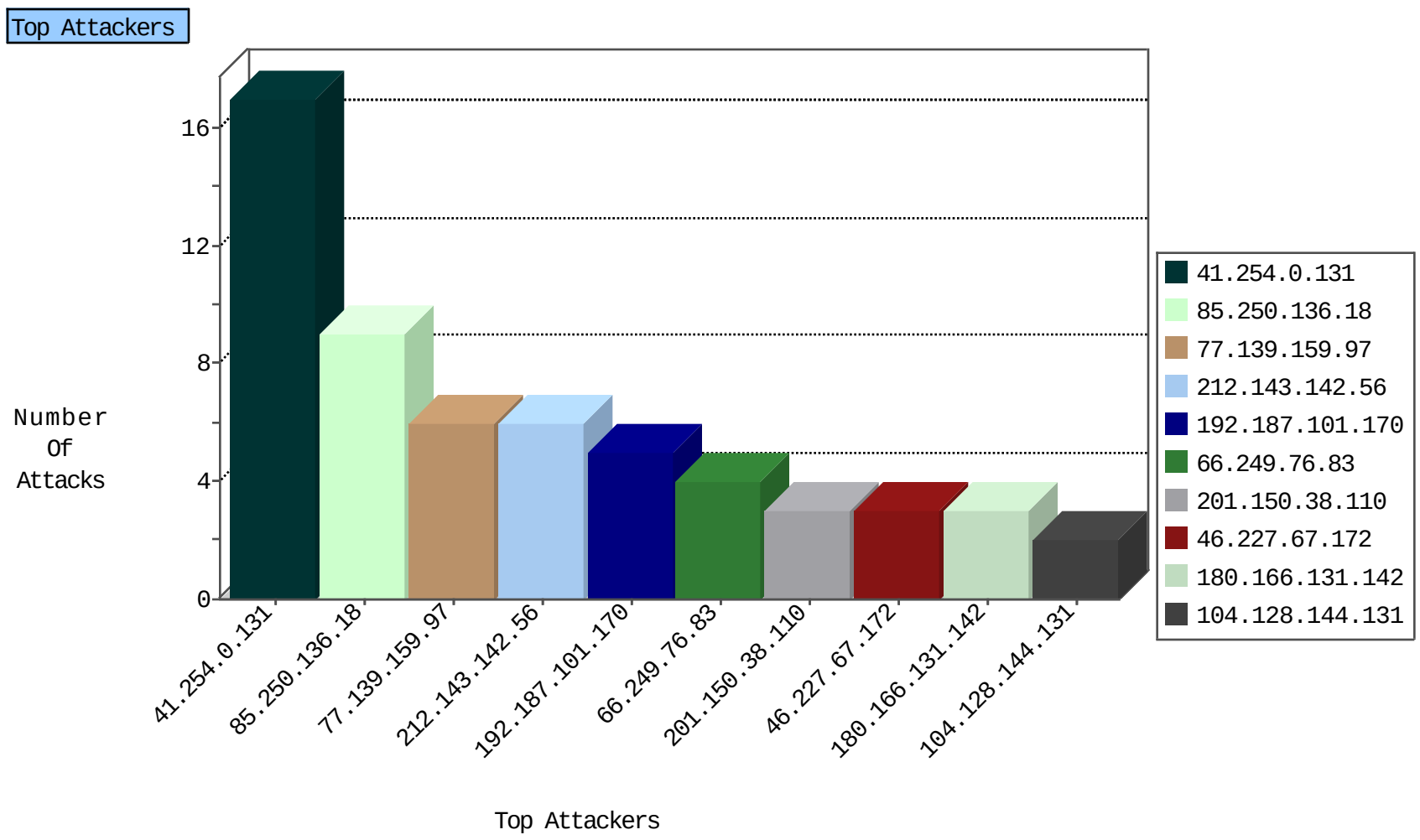
09-03-2016-03:04:06 to 09-03-2016-04:04:06

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-03-2016-03:04:06 to 09-03-2016-04:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.139.159.97	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15
85.250.136.18	Israel	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	9
124.44.66.53	Japan	147.237.76.42	refuah.idf.il	Black List	drop	1
141.212.122.111	United States	147.237.76.201	e.atal.idf.il	Black List	drop	1
217.23.9.123	Netherlands	147.237.76.30	himush.idf.il	Black List	drop	1

09-03-2016-03:04:06 to 09-03-2016-04:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-03-2016-03:04:06 to 09-03-2016-04:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
180.166.131.142	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
119.207.126.67	147.237.76.34	Korea, Republic of	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.128.144.131	147.237.76.199	Canada	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.52.71	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
212.224.109.179	147.237.76.147	Germany	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
201.150.38.110	147.237.77.205	Mexico	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
46.227.67.172	147.237.77.227	Sweden	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
191.109.12.91	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.227.67.172	147.237.77.178	Sweden	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
186.115.110.139	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
14.39.190.129	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.166.131.142	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
180.96.11.23	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
106.186.20.183	147.237.0.19	Japan	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
104.128.144.131	147.237.76.199	Canada	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
94.102.52.71	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
201.150.38.110	147.237.77.205	Mexico	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
94.102.48.195	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
201.150.38.110	147.237.77.205	Mexico	prisha.idf.il	ET SCAN NMAP -f -sS	1
46.227.67.172	147.237.77.205	Sweden	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
186.115.110.139	147.237.77.178	Colombia	e.matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
180.166.131.142	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1

09-03-2016-03:04:06 to 09-03-2016-04:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
41.254.0.131	Libyan Arab Jamahiriya	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	16
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
103.4.123.34	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.30	United States	147.237.0.33	idf.il	drop		drop	1
141.212.122.31	United States	147.237.0.33	idf.il	drop		drop	1
41.254.0.131	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

09-03-2016-03:04:06 to 09-03-2016-04:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.187.101.170	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.187.101.170	Block	4
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.69.67	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
207.46.13.191	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
192.187.101.170	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/admin/elfinder/elfinder.html	Block	1
66.249.69.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-he/refuah.aspx	Block	1
68.180.229.39	United States	147.237.76.31	nakchal.idf.i	Parameter Type Violation PageNum in www.nakhal.idf.il/1111-he/nakhal.aspx	Block	1
192.243.55.135	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/mesiratmeida	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
121.7.37.132	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
198.20.69.74	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/robots.txt	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
176.9.10.227	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/tikshuv/index.htm-אתר	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
204.79.180.100	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1

09-03-2016-03:04:06 to 09-03-2016-04:04:06