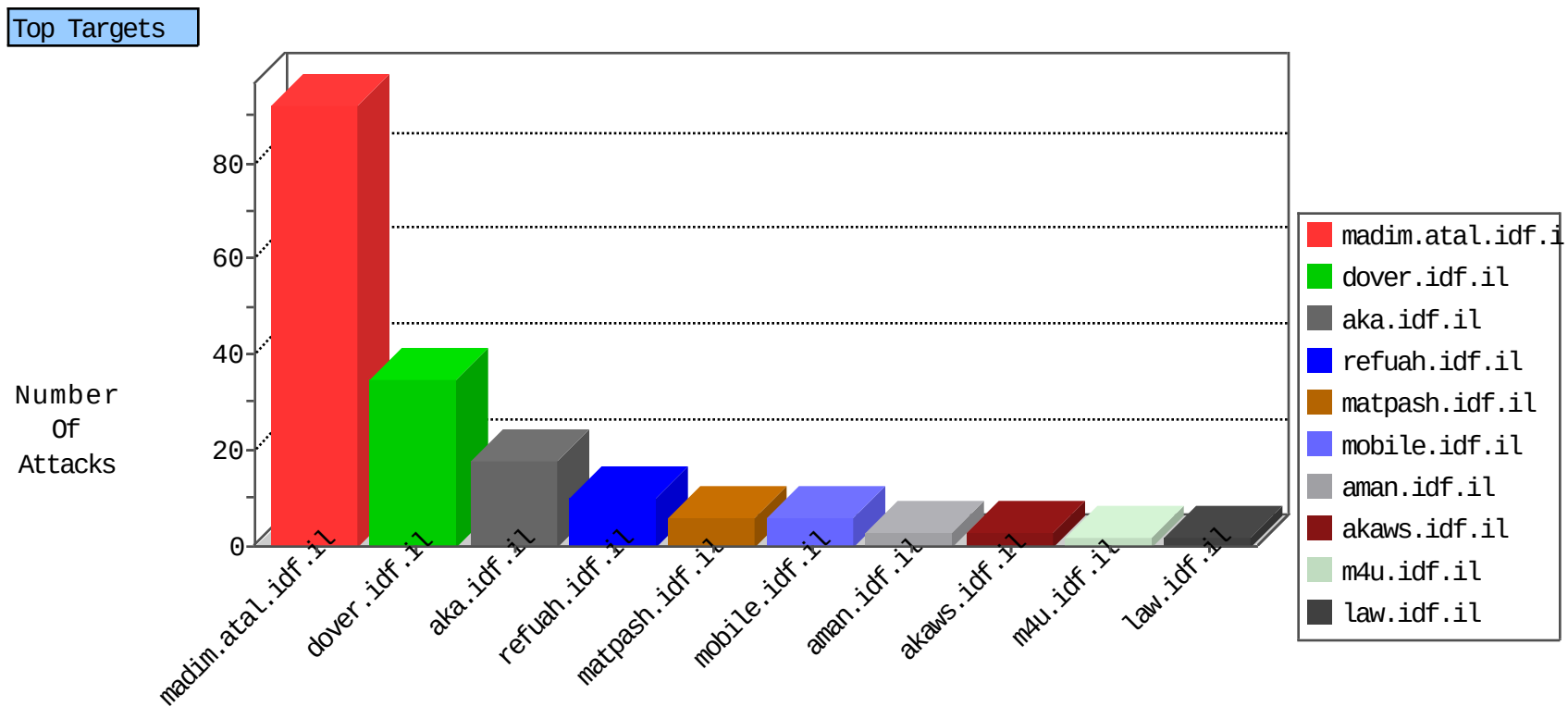
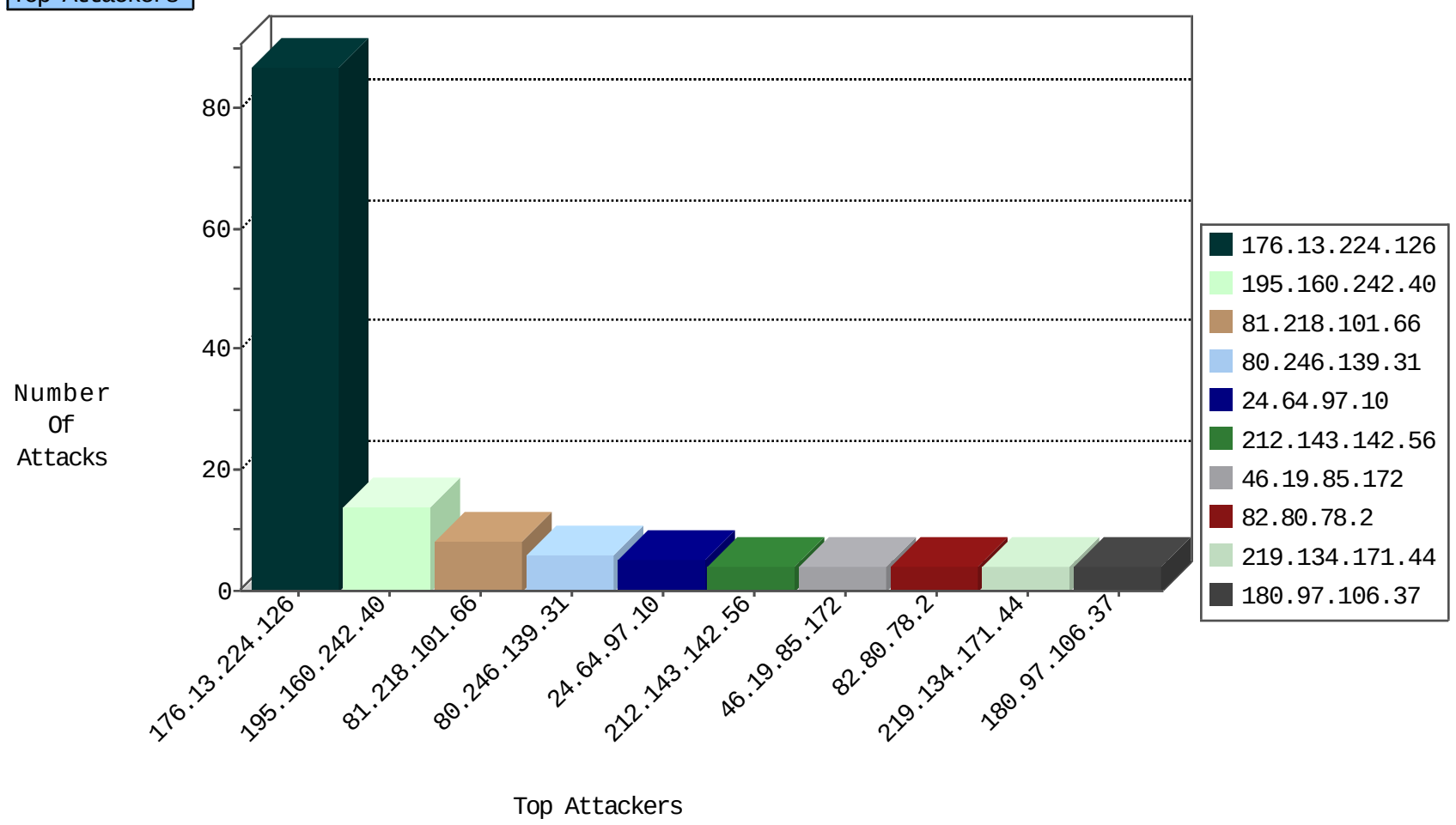
08-18-2016-07:04:01 to 08-18-2016-08:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-18-2016-07:04:01 to 08-18-2016-08:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	3
176.13.224.126	Israel	147.237.0.19	madim.atal.idf.il	DOSS-SSL-ClearText	drop	1
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	1

08-18-2016-07:04:01 to 08-18-2016-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
86.186.225.159	United Kingdom	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-18-2016-07:04:01 to 08-18-2016-08:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
186.170.132.143	147.237.0.35	Colombia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.118.65.230	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
162.216.19.183	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
91.201.236.50	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
54.79.2.19	147.237.77.176	Australia	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
185.118.65.230	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN Potential SSH Scan	1
162.216.19.183	147.237.77.216	United States	dover.idf.il	SERVER-WEBAPP TRACE attempt	1
109.64.182.48	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.218.204.245	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1

08-18-2016-07:04:01 to 08-18-2016-08:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
81.218.101.66	Israel	147.237.76.42	refuah.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	4
24.64.97.10	Canada	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.172	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.18.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
50.136.242.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.37	China	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
180.97.106.162	China	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
180.97.106.37	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
185.130.6.49	Lithuania	147.237.0.35	akaws.idf.il	drop		drop	1
113.108.10.31	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
180.97.106.37	China	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
176.13.10.57	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.37	China	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1

08-18-2016-07:04:01 to 08-18-2016-08:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.224.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
80.246.139.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	6
37.26.149.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.138.45.93	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	2
2.53.52.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
219.134.171.44	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 219.134.171.44	Block	2
109.67.172.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.22.177	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
2.53.190.11	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.9	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
83.149.37.36	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
219.134.171.44	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/contact.asp	Block	1
138.134.102.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
2.55.137.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.199.151.137	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method POST for www.eitan.aka.idf.il/1103-he/eitan.aspx	None	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
46.19.86.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
77.237.138.202	Czech Republic	147.237.77.74	law.idf.il	Unauthorized URL Access to /	Block	1
12.37.166.70	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
213.8.71.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.8.71.26	Block	1
100.35.75.114	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/forms.aspx	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
180.76.15.29	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
79.177.228.66	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/login.aspx	Block	1
24.64.97.10	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotfaq.aspx	Block	1
104.128.144.131	Canada	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/redirect.php	Block	1
77.138.22.177	France	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
2.53.161.224	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
180.76.15.144	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list7.htm	Block	1
24.130.83.124	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	1
219.134.171.44	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1

08-18-2016-07:04:01 to 08-18-2016-08:04:01