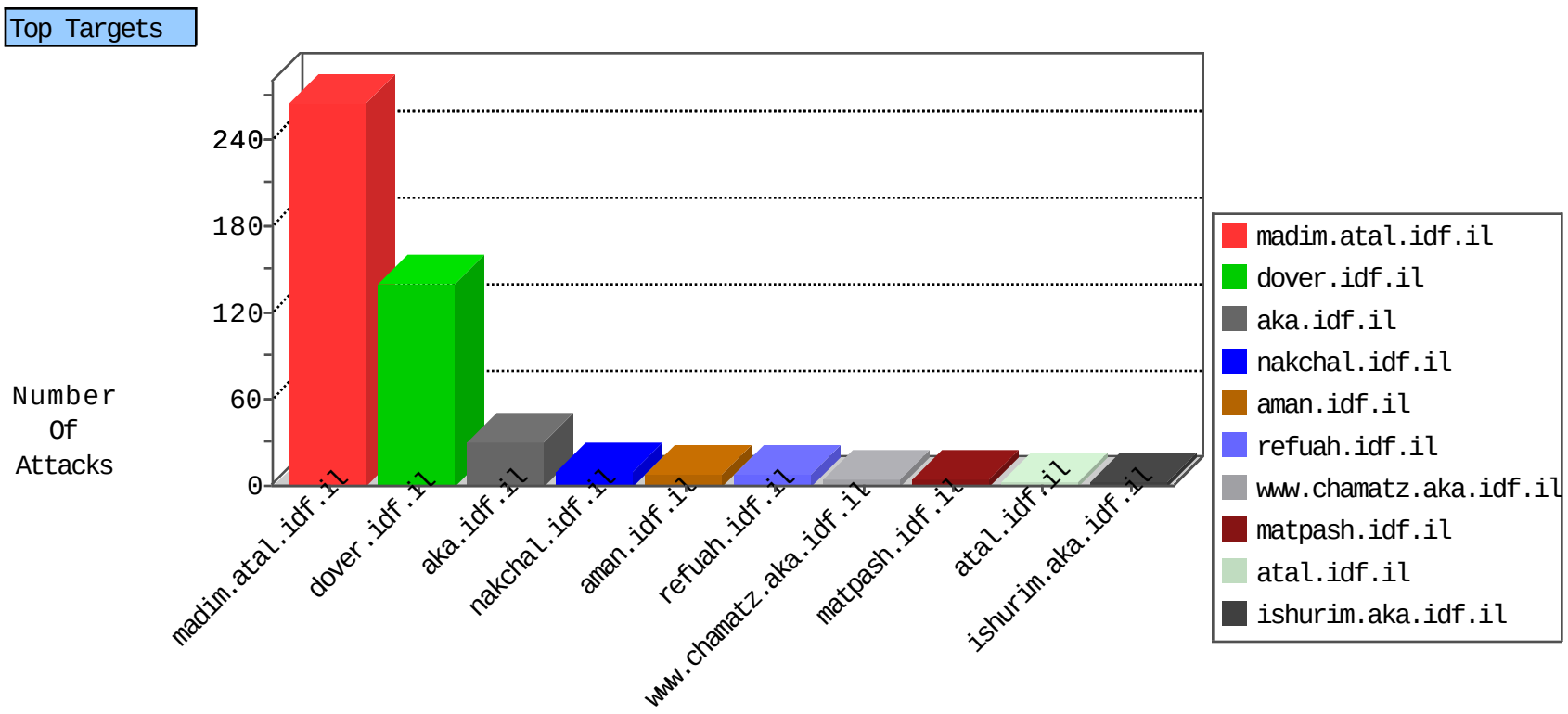
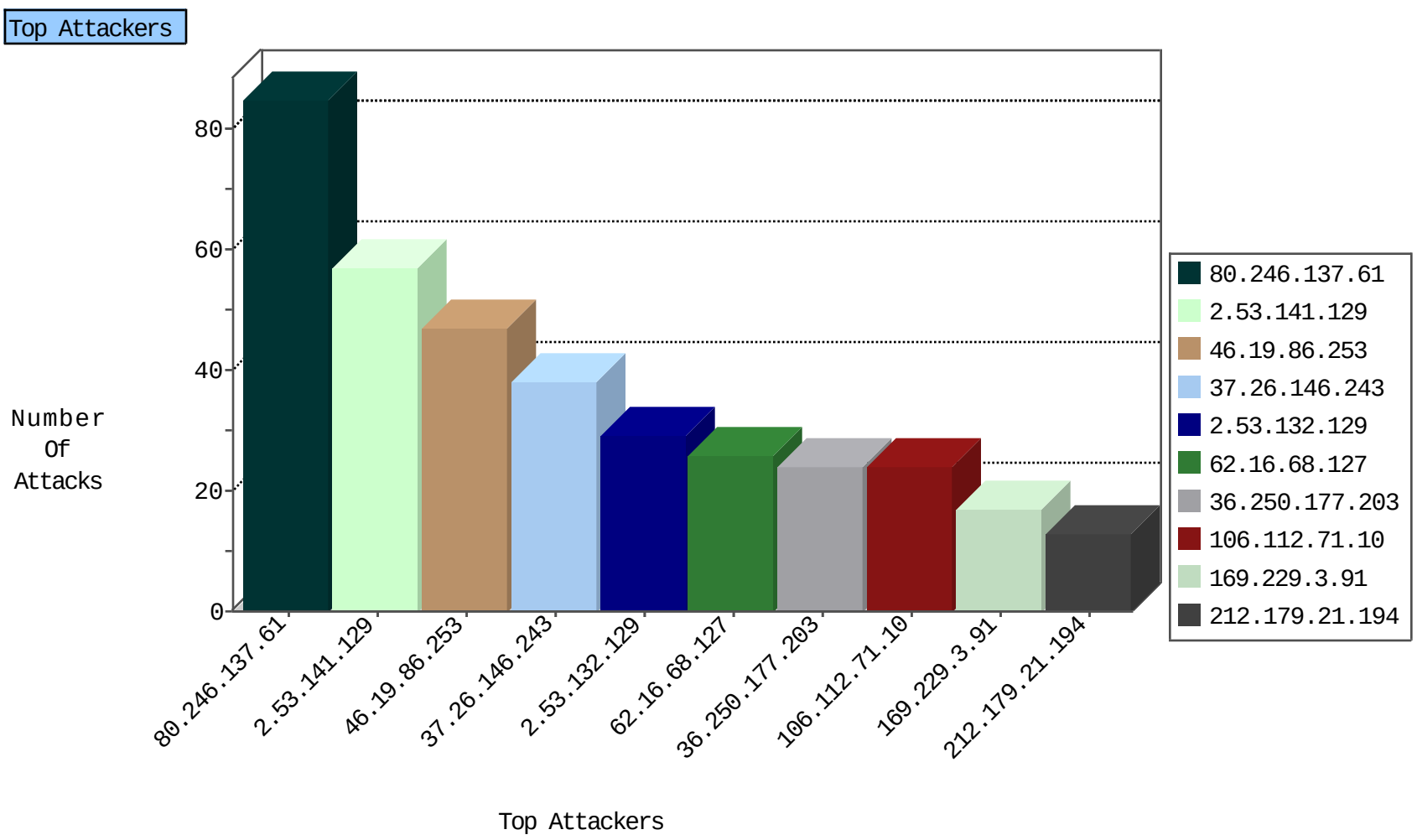
08-18-2016-11:04:00 to 08-18-2016-12:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-18-2016-11:04:00 to 08-18-2016-12:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.92.126	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	10
82.81.90.11	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
93.158.200.131	Netherlands	147.237.76.200	eitan.aka.idf.i	Black List	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
109.64.135.160	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

08-18-2016-11:04:00 to 08-18-2016-12:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-18-2016-11:04:00 to 08-18-2016-12:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
97.105.173.114	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.146	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.126.70.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

08-18-2016-11:04:00 to 08-18-2016-12:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.16.68.127	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
82.80.142.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
88.202.218.230	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
62.16.68.127	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
77.139.246.233	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
87.69.27.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.107.128.101	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
180.97.106.37	China	147.237.76.199	e.nakchal.idf.il	drop	SAM rule	drop	1
109.253.157.13	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
66.249.76.35	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.161	China	147.237.76.196	e.sviva.idf.il	drop	SAM rule	drop	1
176.13.14.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.37	China	147.237.77.227	e.hamaz.idf.il	drop	SAM rule	drop	1
109.253.215.138	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.8.14	e.orchot.idf.il	drop	SAM rule	drop	1
176.13.238.144	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.37	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
109.253.223.75	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
180.97.106.37	China	147.237.8.28	e.mobile-ks.idf.il	drop	SAM rule	drop	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
212.235.64.137	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.161	China	147.237.8.24	e.lifestyle.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.0.200	m4u.idf.il	drop		drop	1
180.97.106.162	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
180.97.106.37	China	147.237.76.44	e.refuah.idf.il	drop	SAM rule	drop	1
109.253.140.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.161	China	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
82.81.90.12	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
212.117.136.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-18-2016-11:04:00 to 08-18-2016-12:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.137.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
2.53.141.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
46.19.86.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
37.26.146.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
2.53.132.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
36.250.177.203	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 36.250.177.203	Block	17
106.112.71.10	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 106.112.71.10	Block	17
156.208.208.140	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	8
36.250.177.203	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
106.112.71.10	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
209.88.198.1	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
109.65.169.86	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
37.26.147.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.109.202.86	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
2.53.148.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
193.106.52.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	2
79.131.190.161	Greece	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.86.114	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
109.253.128.34	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
82.13.92.244	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus	Block	2
2.53.141.129	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/mobile/login.aspx	Block	2
109.253.228.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.139.52.166	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
46.19.86.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
89.139.52.166	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
80.214.73.253	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/cityofficers/	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
66.102.9.105	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/	Block	1
213.208.185.54	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
103.27.126.210	Hong Kong	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Unknown HTTP Request Method ôåjœ[[#11]][[#26]]•cËÕ8éD~e…{q–8(Çóz`t[[#20]]—q›[[#16]]s°q[[#8]],!Á˜þC¡@@[[#7]]A[[#12]][[#7]]I–>Æ•[[#5]]úE!x¿óy• in URL	Block	1
109.67.149.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
91.194.238.31	Ukraine	147.237.72.166	aka.idf.il	Malformed URL eywa.tns-counter.ru:443	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/back.png	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
156.209.38.230	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.180	Israel	147.237.76.42	refuah.idf.il	Distributed Abnormally Long Request	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
85.74.206.75	Greece	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/	Block	1
79.176.53.168	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 79.176.53.168	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Abnormally Long Request method	Block	1
46.19.86.148	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
91.194.238.31	Ukraine	147.237.77.216	dover.idf.il	Malformed URL eywa.tns-counter.ru:443	Block	1
36.250.177.203	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
2.53.28.212	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Unknown HTTP Request Method [[#26]]±<•åNÃ€byþ4[[#1]]C0Ó?Vt'#012[[#21]]]·ñ•K:¼[[#5]]t in URL	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Abnormally Long Request method	Block	1
69.171.228.123	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/0/2950.pdf&usg=afqjcnfrhcwnhkt5t7bz2eyz4fvzwd_xsq	Block	1

08-18-2016-11:04:00 to 08-18-2016-12:04:00