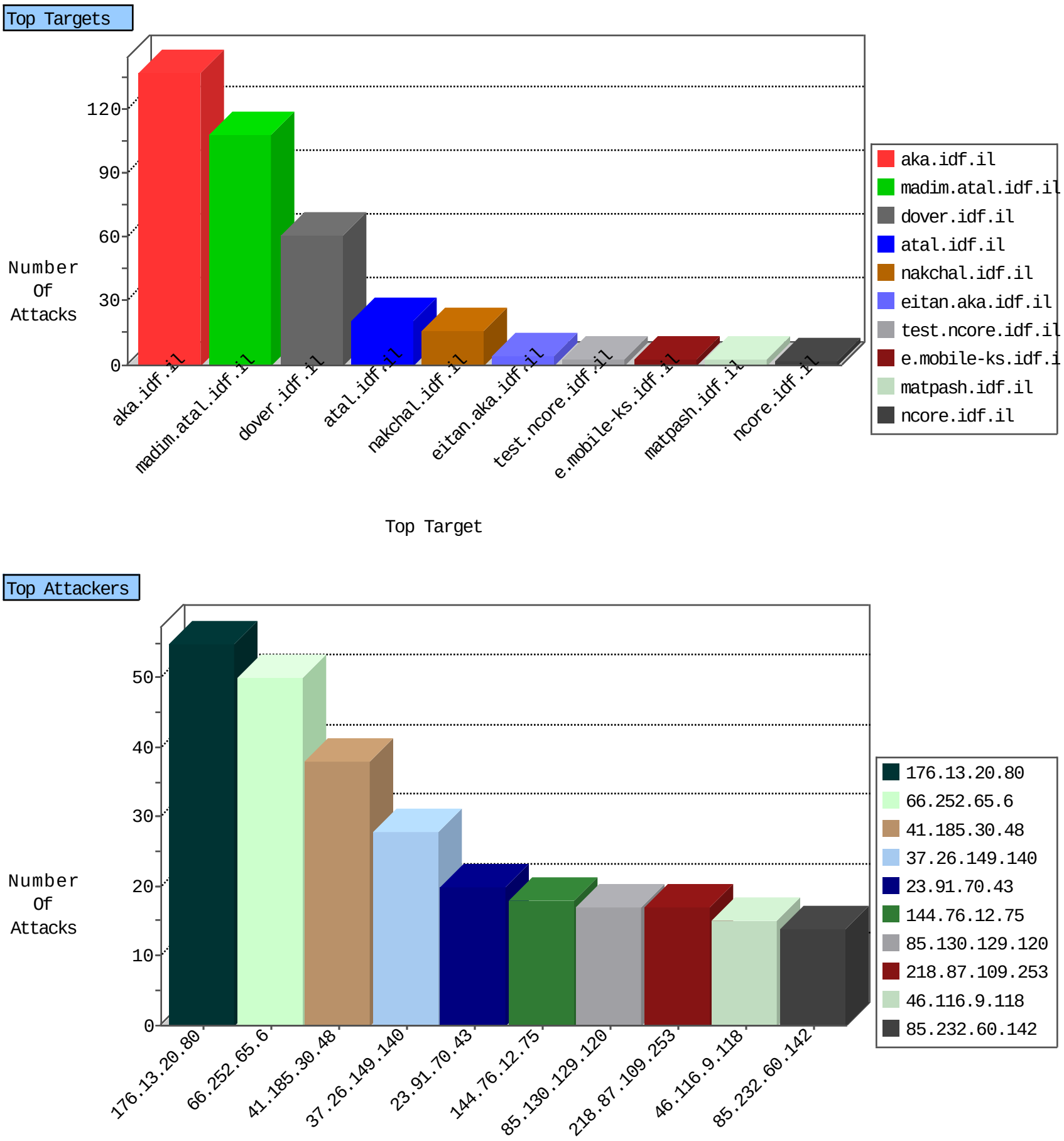
08-19-2016-12:04:03 to 08-19-2016-13:04:03

IDF Under Attack
Daily Report



08-19-2016-12:04:03 to 08-19-2016-13:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.2	United States	147.237.76.176	test.ncore.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.177	ncore.idf.il	Black List	drop	2
185.40.87.243	Turkey	147.237.8.27	e.madim.atal.idf.il	L4 Source or Dest Port Zero	drop	1
185.40.87.243	Turkey	147.237.76.31	nakchal.idf.il	L4 Source or Dest Port Zero	drop	1
185.40.87.243	Turkey	147.237.77.61	e.cogat.idf.il	L4 Source or Dest Port Zero	drop	1
179.32.73.79	Colombia	147.237.77.243	mobile.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

08-19-2016-12:04:03 to 08-19-2016-13:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.252.65.6	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	18
41.185.30.48	South Africa	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
144.76.12.75	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	7
209.15.196.170	Canada	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
41.185.30.48	South Africa	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
85.232.60.142	United Kingdom	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
66.252.65.6	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.43	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
162.210.196.129	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
144.76.12.75	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	3
144.76.12.75	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
144.76.12.75	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
144.76.12.75	Germany	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
23.91.70.43	United States	147.237.77.233	atal.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1
80.169.91.26	United Kingdom	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-19-2016-12:04:03 to 08-19-2016-13:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.252.65.6	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	26
41.185.30.48	147.237.72.166	South Africa	aka.idf.il	SQL Injection - Select From	20
23.91.70.43	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	14
209.15.196.170	147.237.72.166	Canada	aka.idf.il	SQL Injection - Select From	8
85.232.60.142	147.237.72.166	United Kingdom	aka.idf.il	SQL Injection - Select From	8
218.87.109.253	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
87.236.194.161	147.237.77.227	Czech Republic	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
218.87.109.253	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
167.0.176.177	147.237.0.35	Colombia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.87.109.253	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.62.214.201	147.237.8.28	Taiwan	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.87.109.253	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
222.186.58.235	147.237.0.200	China	m4u.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
218.87.109.253	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
218.87.109.253	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
191.32.145.117	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

08-19-2016-12:04:03 to 08-19-2016-13:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.116.9.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
85.130.129.120	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	11
85.130.129.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.23.21	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
136.243.152.18	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.178.254.224	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
91.209.51.22	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
176.13.14.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.200	m4u.idf.il	drop		drop	1
176.13.242.100	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
35.87.255.225	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-19-2016-12:04:03 to 08-19-2016-13:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.20.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
37.26.149.140	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
2.55.36.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
137.132.3.12	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	9
37.26.146.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
84.109.118.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.10.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.76.51	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
185.27.106.161	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
5.29.249.84	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.243.23	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
66.102.9.95	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
93.109.253.38	Cyprus	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 93.109.253.38	Block	1
66.249.76.51	Israel	147.237.72.166	aka.idf.il	Unknown Parameter list in www.aka.idf.il/sites/skira/default.asp	None	1
204.79.180.123	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/home.asp	Block	1
137.132.250.8	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.178.155.65	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
66.249.64.142	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
93.109.253.38	Cyprus	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
68.180.229.39	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
207.46.13.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
144.76.12.75	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 144.76.12.75	Block	1
66.249.66.173	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
176.13.236.131	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	1
117.215.180.91	India	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
74.91.23.166	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
46.19.86.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
144.76.12.75	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13885-en/dover.aspx	Block	1
66.249.66.176	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
185.27.105.135	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
117.215.180.91	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
74.91.23.166	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.102.9.76	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
157.55.39.24	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/default.aspx	Block	1

08-19-2016-12:04:03 to 08-19-2016-13:04:03