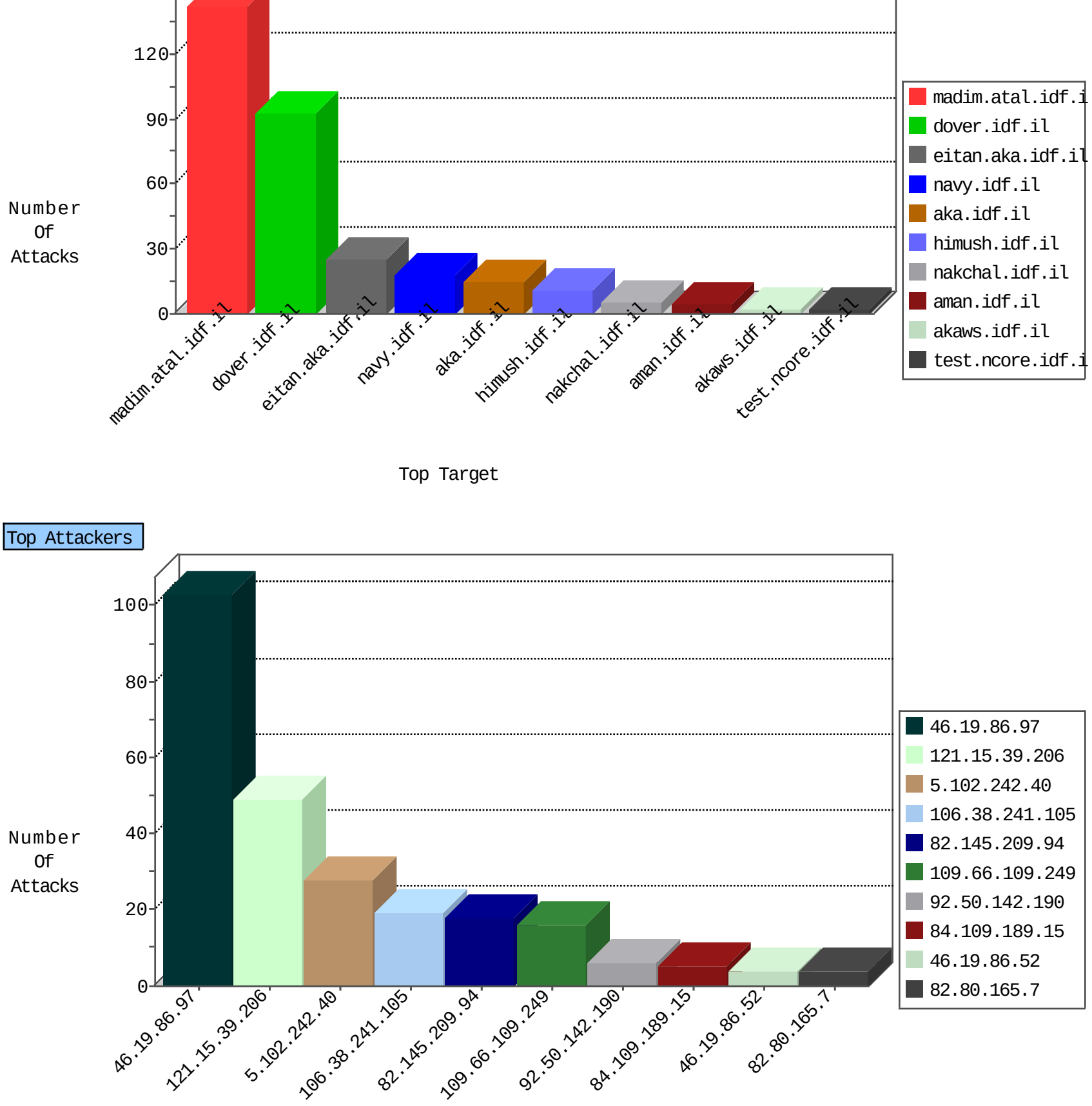
08-19-2016-11:04:03 to 08-19-2016-12:04:03

IDF Under Attack Daily Report



08-19-2016-11:04:03 to 08-19-2016-12:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.209.94	Europe	147.237.76.86	navy.idf.il	Black List	drop	18
46.19.86.120	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
115.230.125.146	China	147.237.76.176	test.ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
66.240.219.146	United States	147.237.76.34	yohalan.idf.il	Black List	drop	1
115.230.125.146	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
71.6.146.185	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
167.0.228.48	Colombia	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

08-19-2016-11:04:03 to 08-19-2016-12:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	19

08-19-2016-11:04:03 to 08-19-2016-12:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
58.218.204.245	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.76.39	United States	mobile.meitav.idf.i	ET DROP Dshield Block Listed Source	1
183.82.106.200	147.237.77.179	India	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
139.162.13.205	147.237.76.30	Singapore	himush.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
186.115.38.17	147.237.0.35	Colombia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.82.106.200	147.237.77.179	India	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1

08-19-2016-11:04:03 to 08-19-2016-12:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.66.109.249	Israel	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	8
109.66.109.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
92.50.142.190	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.71.171.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
82.207.91.242	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.109.189.15	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.181.104.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
82.80.165.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
117.198.194.204	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
188.247.73.138	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.181.96.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.195.168	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.76.201	e.atal.idf.il	drop	SAM rule	drop	1
109.66.109.249	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
2.53.45.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.198.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	1
176.13.22.145	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.76.198	e.yohalan.idf.il	drop	SAM rule	drop	1

08-19-2016-11:04:03 to 08-19-2016-12:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	103
5.102.242.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
121.15.39.206	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 121.15.39.206	Block	17
121.15.39.206	China	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 121.15.39.206	Block	17
121.15.39.206	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
121.15.39.206	China	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	6
2.55.27.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.57.177.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.116.52.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.80.165.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.22.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.179.161.94	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
46.229.164.102	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
176.228.44.95	Israel	147.237.77.74	law.idf.il	Parameter Type Violation FreeText in www.mag.idf.il/421-he/patzar.aspx	Block	1
121.15.39.206	China	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/	None	1
79.179.161.94	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
66.249.76.52	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	1
138.134.102.15	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
93.172.197.18	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
79.178.237.94	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.102.9.20	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
185.3.147.113	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
121.15.39.206	China	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/index.asp	Block	1
77.138.135.45	France	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/	Block	1
139.162.13.205	Singapore	147.237.76.30	himush.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
93.173.238.217	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.179.1.13	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.102.9.85	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
204.79.180.176	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
84.109.189.15	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
77.139.38.52	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
139.162.13.205	Singapore	147.237.76.30	himush.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.179.161.94	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.179.161.94	Block	1
66.249.66.182	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/894-he	Block	1
87.69.164.38	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 87.69.164.38 (Open Mode)	None	1
77.139.88.190	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
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
121.15.39.206	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
90.182.178.182	Czech Republic	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
79.178.12.199	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized Method HEAD for www.chinuch.aka.idf.il/894-he/chinuch.aspx	None	1

08-19-2016-11:04:03 to 08-19-2016-12:04:03