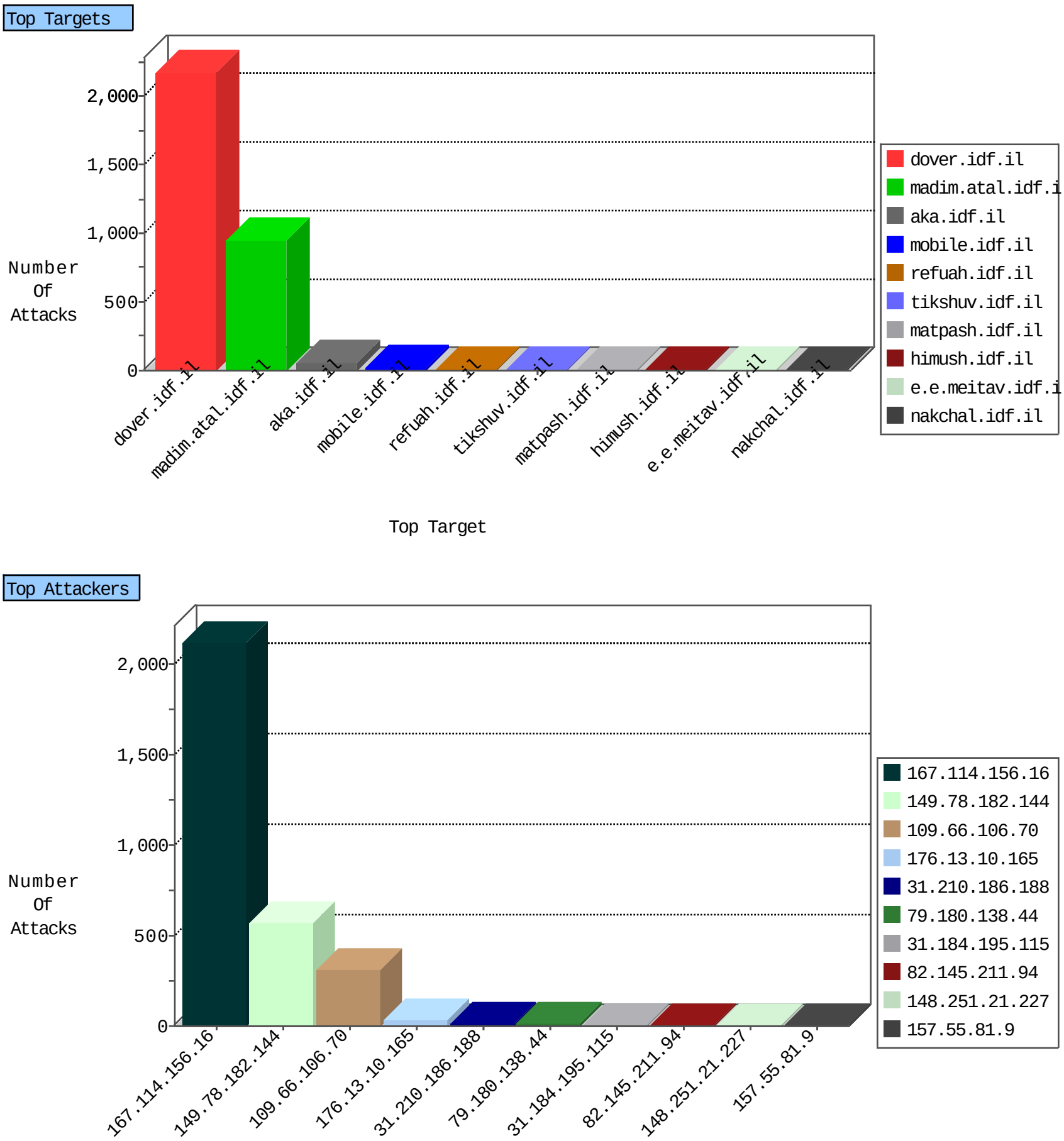
01-04-2016-22:04:05 to 01-04-2016-23:04:05

IDF Under Attack Daily Report



01-04-2016-22:04:05 to 01-04-2016-23:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3456
82.145.211.94	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	7
157.55.81.9	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
109.64.67.57	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
155.94.207.42	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1

01-04-2016-22:04:05 to 01-04-2016-23:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.245	Israel	147.237.77.176	matpash.idf.il	14170: HTTP: Blank User-Agent (descriptor but no string)	Block	1

01-04-2016-22:04:05 to 01-04-2016-23:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.246.130.132	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
31.184.195.115	147.237.0.33	Russian Federation	idf.il	ET SCAN Potential SSH Scan	1
115.182.249.11	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
14.162.117.57	147.237.76.31	Vietnam	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.241.28.82	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.39.222.253	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
109.64.181.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.154.60.27	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	1
40.115.58.160	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
192.186.95.178	147.237.0.15	Canada	kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
31.184.195.115	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
31.184.195.115	147.237.72.217	Russian Federation	e.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
31.184.195.115	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
117.25.155.164	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.195.115	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
115.182.249.11	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
12.139.41.189	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
109.66.179.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.68.44.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.12.39.85	147.237.76.38	Russian Federation	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
62.75.236.76	147.237.8.27	Germany	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.195.115	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
192.186.95.178	147.237.0.15	Canada	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
31.184.195.115	147.237.76.147	Russian Federation	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
31.184.195.115	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN Potential SSH Scan	1
117.25.155.164	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 3072	1

01-04-2016-22:04:05 to 01-04-2016-23:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count

01-04-2016-22:04:05 to 01-04-2016-23:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.182.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	340
109.66.106.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	196
149.78.182.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	126
109.66.106.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	115
149.78.182.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
176.13.10.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
31.210.186.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
79.180.138.44	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
93.172.87.209	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
148.251.21.227	Germany	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	4
46.19.86.86	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.132.211	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
87.69.178.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.179.216.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.147.133	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
172.56.13.255	United States	147.237.77.216	dover.idf.il	Post Request - Missing Content Type	Block	2
46.117.197.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.176.154.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.176	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
149.78.60.68	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.195.227	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.177.117.53	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
211.123.214.30	Japan	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp/wp-admin/	Block	1
109.253.128.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/17012011masaiyot.aspx	Block	1
185.120.126.49		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
81.218.140.112	Israel	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
46.19.86.165	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
149.78.182.144	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
5.28.172.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.112	United States	147.237.0.34	tikshuv.idf.il	Distributed Malformed URL	Block	1
79.180.139.40	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/giyus/general.aspx	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
176.13.13.167	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
87.69.48.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.178.195.236	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
46.19.85.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.136.21	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.195.203	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
212.76.123.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.129.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.96.202	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-12512-he/dover.aspx&sa=u&ved=0ahukewibt4pxgjhkahuee w8khxioaj8qfggnmak&usg=afqjcnf-yzqkyaercjcxqkhkwmazjq-yba	Block	1
66.249.69.50	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/m/main/giyus/general.aspx	Block	1
193.53.83.21	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
82.166.240.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-04-2016-22:04:05 to 01-04-2016-23:04:05