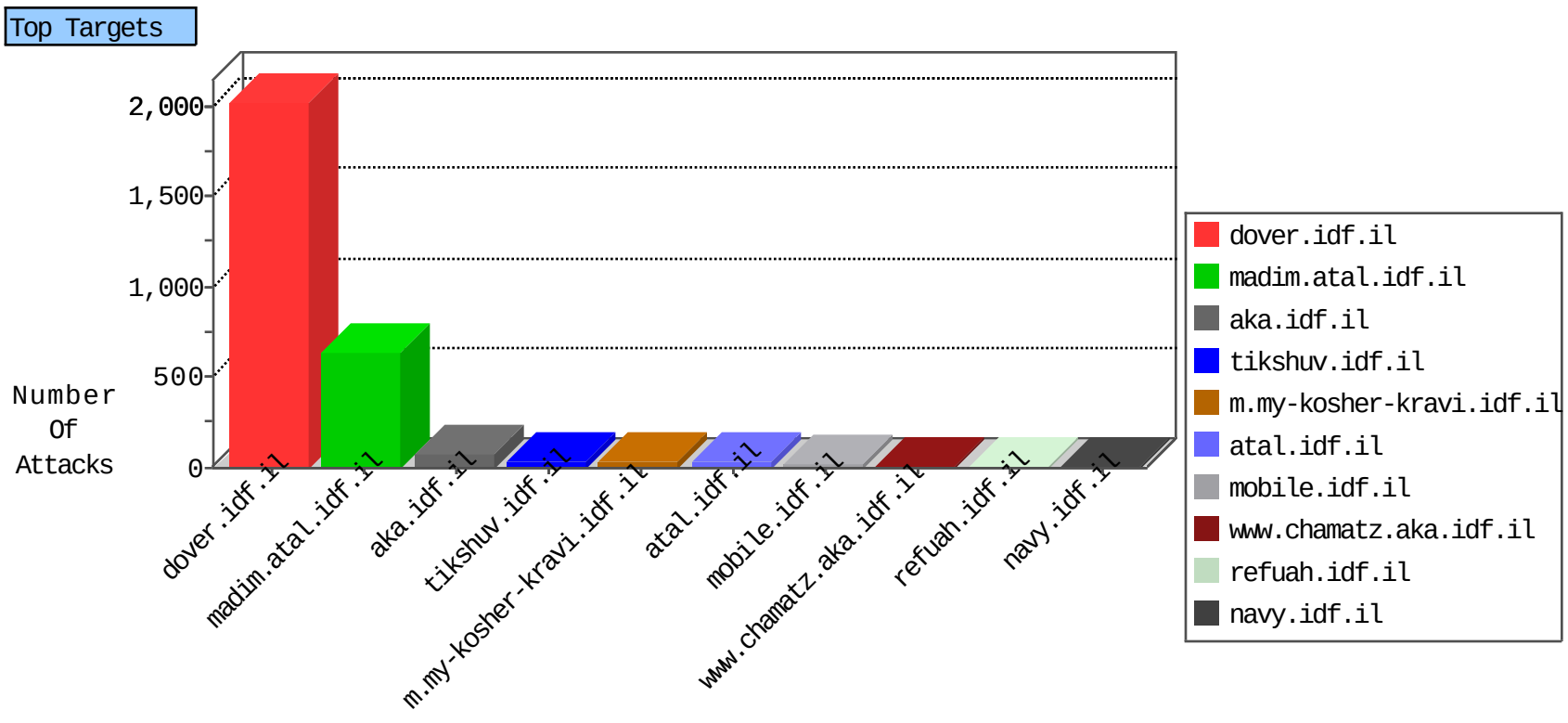
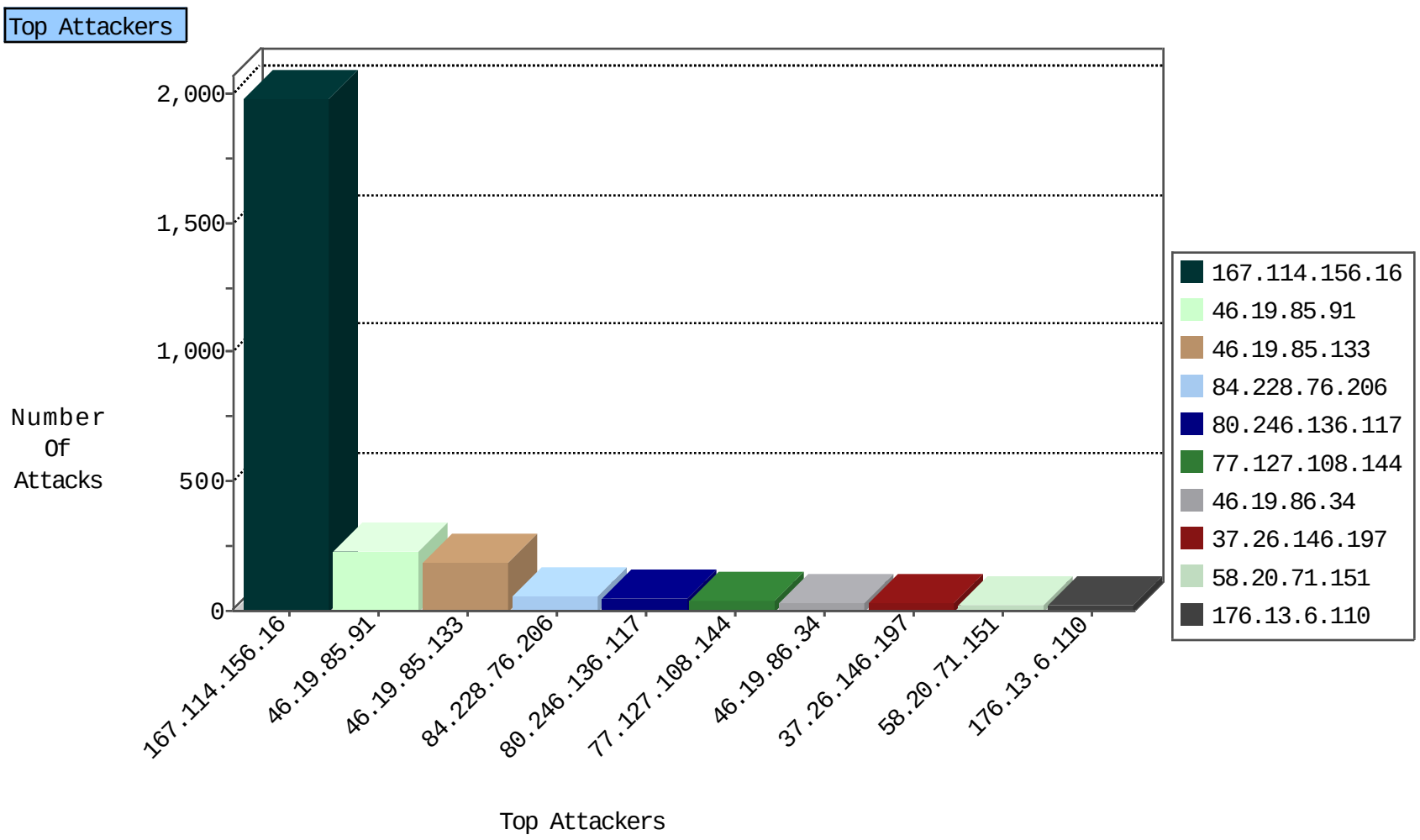
01-04-2016-20:04:05 to 01-04-2016-21:04:05

IDF Under Attack Daily Report





01-04-2016-20:04:05 to 01-04-2016-21:04:05

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	3145
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
109.64.164.194	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
37.26.146.132	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
71.6.216.37	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.39	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
105.198.225.227	Egypt	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.171	Switzerland	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
105.198.225.227	Egypt	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

01-04-2016-20:04:05 to 01-04-2016-21:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-04-2016-20:04:05 to 01-04-2016-21:04:05

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
80.246.133.204	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
66.249.93.145	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
109.253.193.204	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	2
109.253.193.204	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	2
95.129.32.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
210.195.211.233	147.237.77.226	Malaysia	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
80.178.13.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.231	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.231	147.237.76.39		mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.224	147.237.8.50		e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
176.13.4.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
106.75.199.173	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
210.195.211.233	147.237.77.226	Malaysia	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
209.126.116.147	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
77.125.149.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.231	147.237.77.235		sviva.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
185.130.5.231	147.237.76.39		mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.231	147.237.72.166		aka.idf.il	ET SCAN Potential SSH Scan	1
185.45.13.150	147.237.77.176	Romania	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
109.67.131.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.195.211.233	147.237.77.226	Malaysia	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1

01-04-2016-20:04:05 to 01-04-2016-21:04:05

Top Attackers In FW

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

01-04-2016-20:04:05 to 01-04-2016-21:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	166
46.19.85.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.85.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	71
46.19.85.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	68
80.246.136.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
77.127.108.144	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 77.127.108.144	Block	37
84.228.76.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
46.19.86.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
37.26.146.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
176.13.6.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
58.20.71.151	China	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 58.20.71.151	Block	23
37.26.149.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
77.126.30.203	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	15
109.66.120.54	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	11
79.182.3.69	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
109.253.132.139	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation RepeatPassword in mobile.idf.il/sachar/changepassword	Block	7
46.19.85.133	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.133	Block	5
185.3.144.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.176.118.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.148.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.145.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.117.61.28	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
212.143.85.205	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
176.13.9.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.46.55	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
176.13.18.179	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
95.86.95.102	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.95.102	Block	2
95.86.95.102	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/&sa=u&ved=0ahukewjtzoy055dkahxluhqkhxyxdeyqfggimaa&usg=afqjcnh4ucr3bqpmkvh4yz9t7jscutsloq	Block	2
176.13.4.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.230.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
79.176.175.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.120.125.25		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
37.26.146.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.101.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
2.52.188.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.90.4	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	1
217.132.27.101	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.121.96.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.147.34	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
46.19.85.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.113.130	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
201.247.189.22	El Salvador	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
182.66.14.126	India	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
37.142.173.232	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
89.161.164.10	Poland	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
54.88.205.44	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-login.php	Block	1
149.88.76.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-04-2016-20:04:05 to 01-04-2016-21:04:05