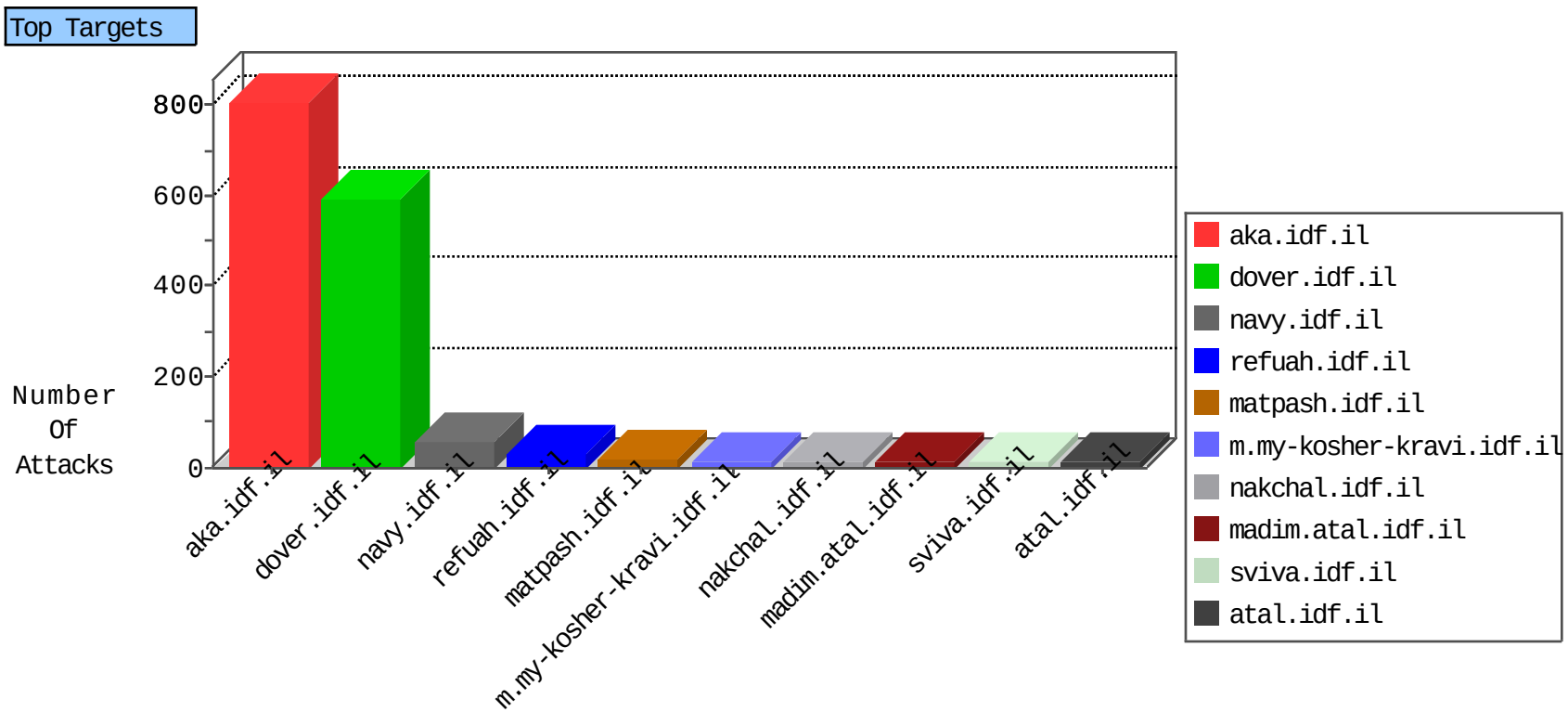
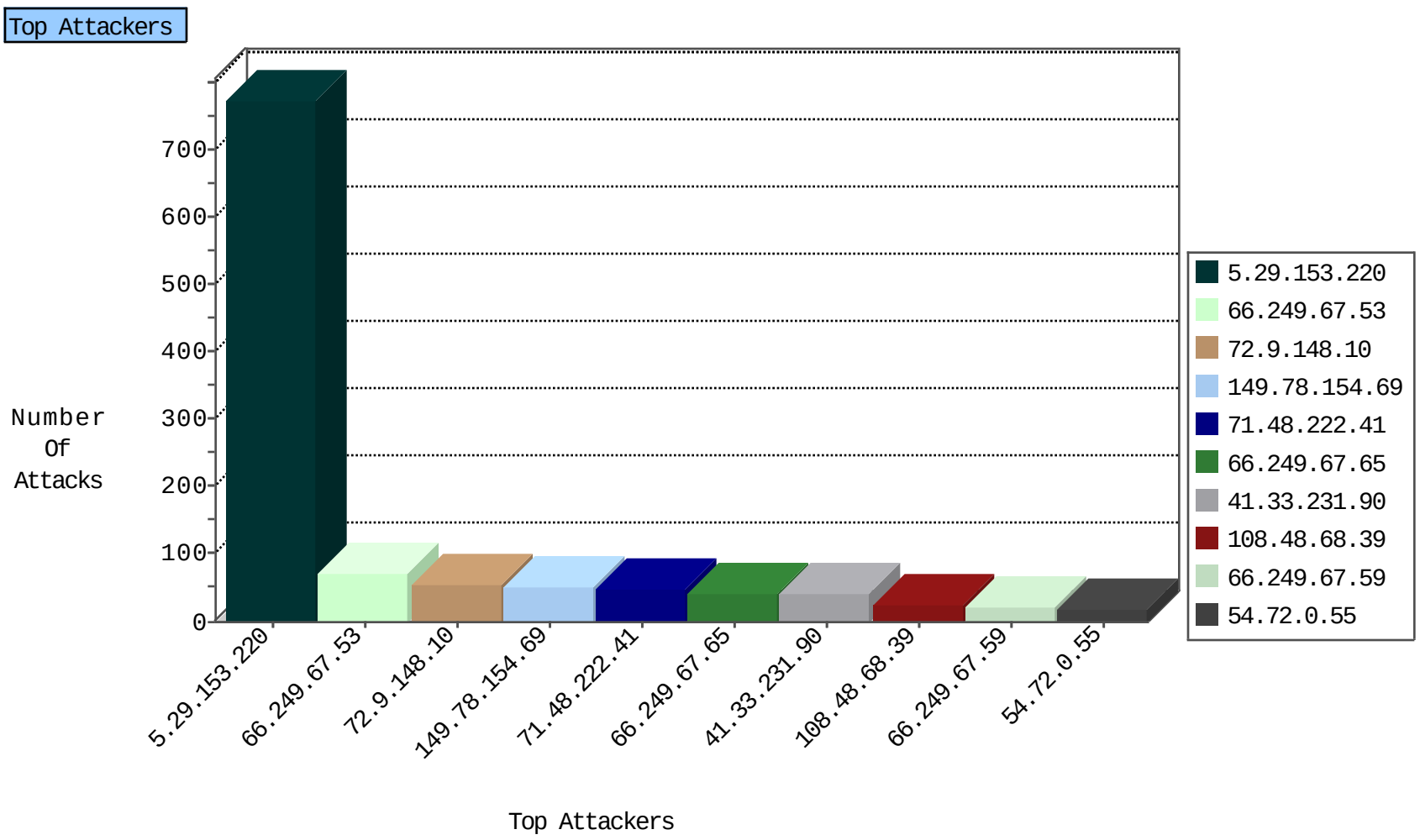
10-26-2015-04:04:09 to 10-26-2015-05:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-26-2015-04:04:09 to 10-26-2015-05:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.153.220	Israel	147.237.72.166	aka.idf.il	TCP Scan (vertical)	drop	3567
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
115.231.222.40	China	147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Http	drop	3
115.231.222.40	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Http	drop	2
141.212.121.198	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	drop	1

10-26-2015-04:04:09 to 10-26-2015-05:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.138.229.119	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

10-26-2015-04:04:09 to 10-26-2015-05:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.29.153.220	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sS window 1024	60
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
178.234.148.13	147.237.77.170	Russian Federation	maarachot.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
132.255.77.72	147.237.8.28		e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.194	147.237.76.200	Netherlands	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.194	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
196.218.155.73	147.237.76.148	Egypt	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 4096	1
132.255.77.72	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
132.255.77.72	147.237.8.24		e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.194	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
78.160.117.58	147.237.76.30	Turkey	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
196.218.155.73	147.237.76.148	Egypt	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 3072	1

10-26-2015-04:04:09 to 10-26-2015-05:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
71.48.222.41	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
108.48.68.39	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
194.187.168.19	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
174.4.17.116	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.12.150.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
157.55.2.139	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
76.115.253.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
47.21.226.138	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.224.149.230	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
118.69.111.76	Vietnam	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
207.241.237.209	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
98.198.41.164	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.235	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
198.58.103.28	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
154.5.154.26	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
77.66.60.74	Denmark	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.67.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.29.70.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.102.8.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
87.69.62.229	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	3
131.253.25.140	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
62.69.162.109	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.228.58.228	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.67.59	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
96.246.232.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.144	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
65.19.138.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.255	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
113.197.14.2	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
38.108.87.20	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
198.58.102.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
98.254.124.78	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

10-26-2015-04:04:09 to 10-26-2015-05:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	56
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.53	Block	42
70.29.38.161	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18774-en/dover.aspxfor	Block	14
173.192.239.226	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1186-he/idfg.aspx&usg=alkjrhhwndmjhm5_lnihdx6b0l_gtbdeda	Block	14
66.249.67.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	14
66.49.225.162	Canada	147.237.77.235	sviva.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	14
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
176.12.141.211	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Double URL Encoding - parameter: ReturnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	14
66.249.67.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
79.180.151.221	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	14
184.105.247.196	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	14
66.249.75.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
104.238.169.129		147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	14
188.165.15.37	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1240-he/atal.aspx	Block	14
66.249.78.4	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	14
157.55.39.255	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.67.77	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	14
62.210.88.201	France	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.google.pl/search	Block	14
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8929-he/refuah.aspx	Block	14

10-26-2015-04:04:09 to 10-26-2015-05:04:09