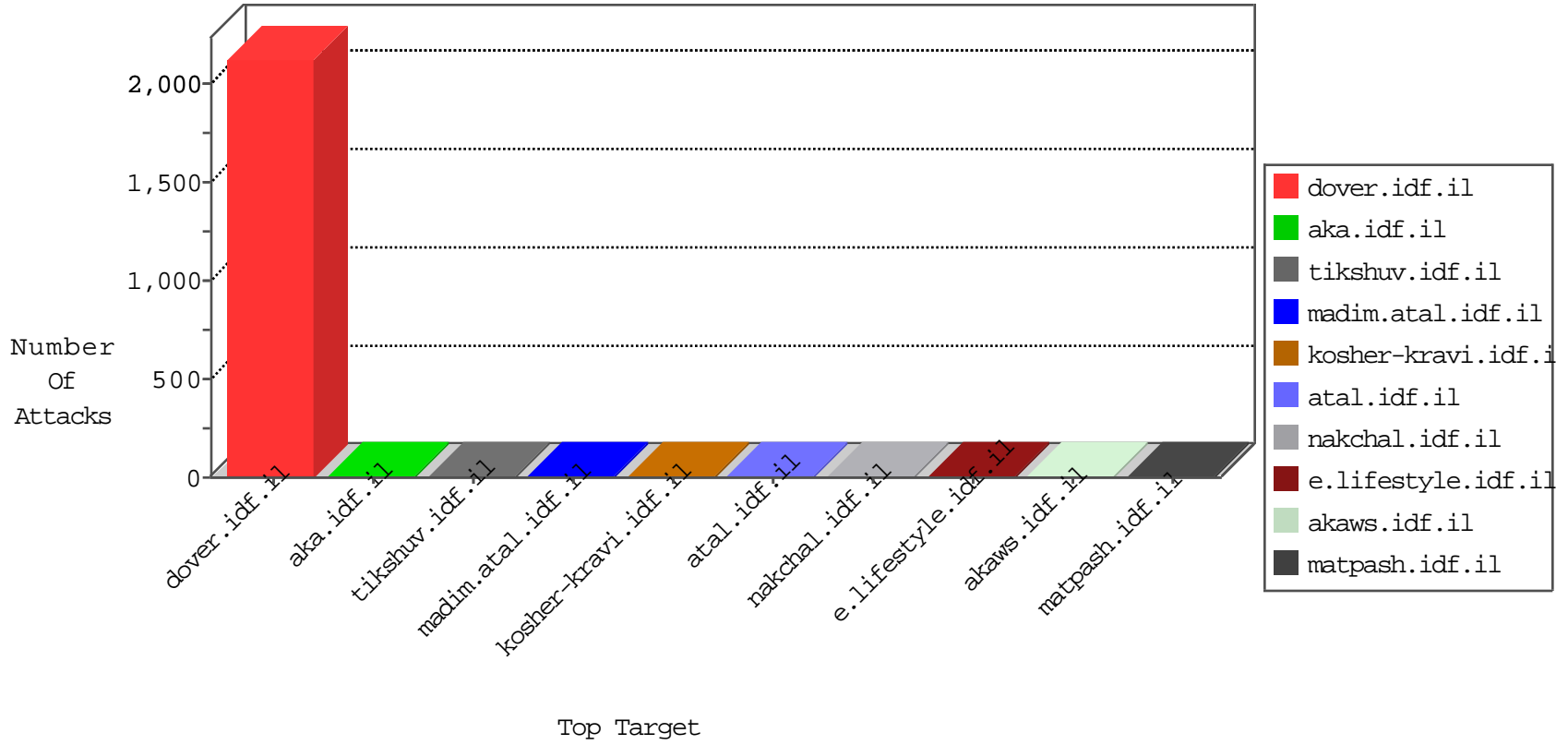


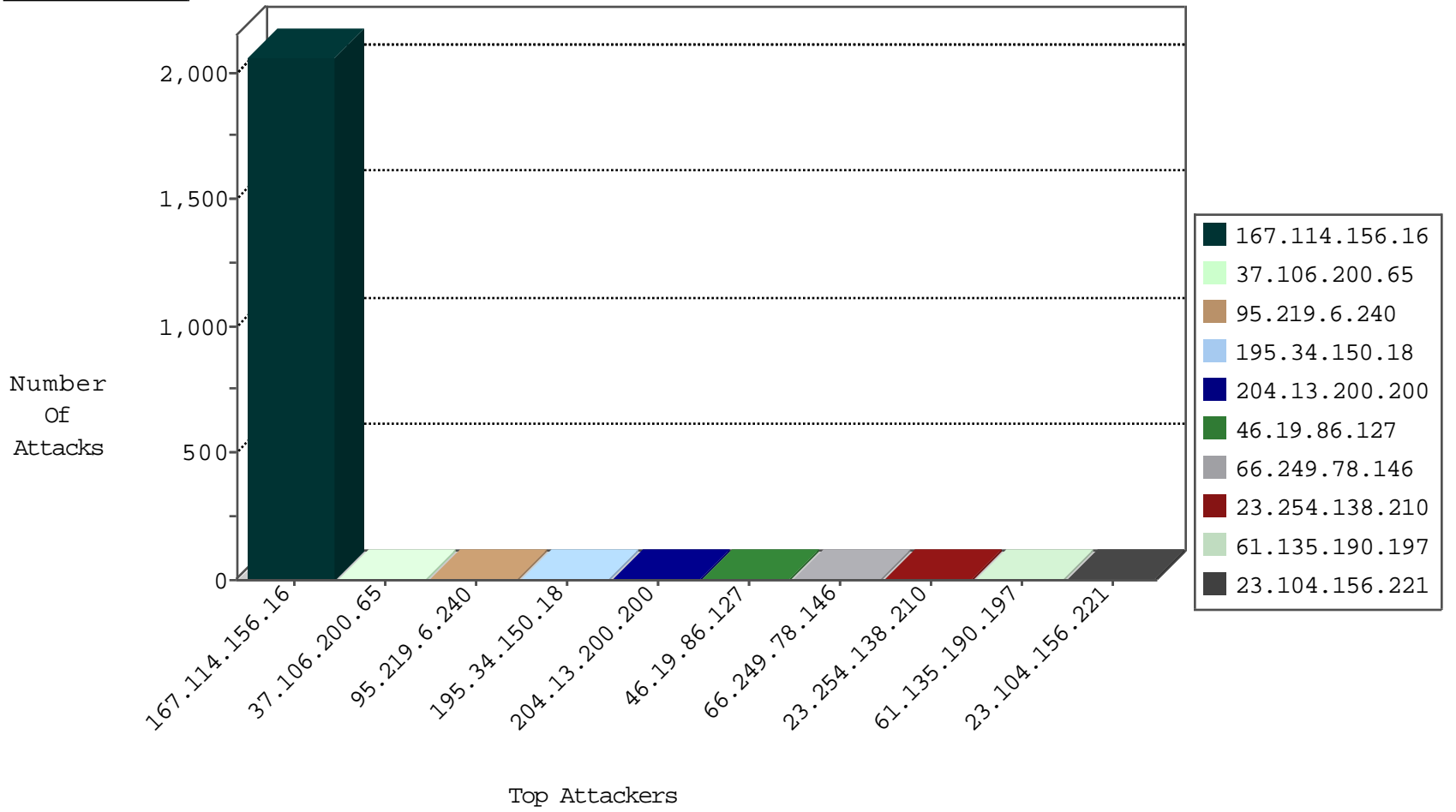
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3143
71.6.216.43	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
52.53.222.9	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
64.246.161.190	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	drop	1

01-05-2016-04:04:07 to 01-05-2016-05:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.144	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
115.124.106.226	India	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

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
66.249.64.238	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
104.140.140.111	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
93.174.93.142	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
83.56.3.111	147.237.76.86	Spain	navy.idf.il	ET SCAN NMAP -sS window 4096	1
209.126.116.147	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.224	147.237.77.233		atal.idf.il	ET SCAN NMAP -sS window 1024	1
104.140.140.111	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
98.119.105.221	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
93.174.93.142	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.106.200.65	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.106.200.65	Block	5
95.219.6.240	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	4
23.254.138.210	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 23.254.138.210	Block	3
46.19.86.127	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
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	2
104.251.91.113		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
61.135.190.69	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/text.css	Block	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
23.104.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/homepage.aspx/templates/social/twitter.aspx	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
61.135.190.198	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/reset.css	Block	1
157.55.39.201	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
104.251.91.113		147.237.77.216	dover.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$ucArticleLobbyControl\$txtSearch in www.idf.il/1283-en/dover.aspx	Block	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/langstyle.css	Block	1
61.135.190.71	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/nav.css	Block	1
23.104.156.221	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/homepage.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
61.135.190.200	China	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
173.252.89.56	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
23.80.153.146	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter ct100\$ContentPlaceHolder1\$ucArticleLobbyControl\$txtSearch	Block	1
104.251.91.165		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/homepage.aspx/templates/social/twitter.aspx	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
61.135.190.72	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/layoutdev.css	Block	1
109.201.152.234	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
23.104.156.221	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
95.219.6.240	Romania	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.219.6.240	Block	1
61.135.190.200	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/layout.css	Block	1
37.106.200.65	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
104.251.91.165		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/homepage.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
23.80.153.146	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	1
61.135.190.197	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
141.212.122.112	United States	147.237.76.31	nakchal.idf.il	Multiple Malformed URL from 141.212.122.112	Block	1
23.106.179.213	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/homepage.aspx/templates/social/twitter.aspx	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19559-he/dover.aspx	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
23.104.156.109	United States	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter ct100\$ContentPlaceHolder1\$ucArticleLobbyControl\$txtSearch	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
61.135.190.197	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/shared/clientscripts/imagevideogallerylobby/imagevideogallerylobby.js	Block	1
23.106.239.65	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/homepage/homepage.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
157.55.39.140	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1