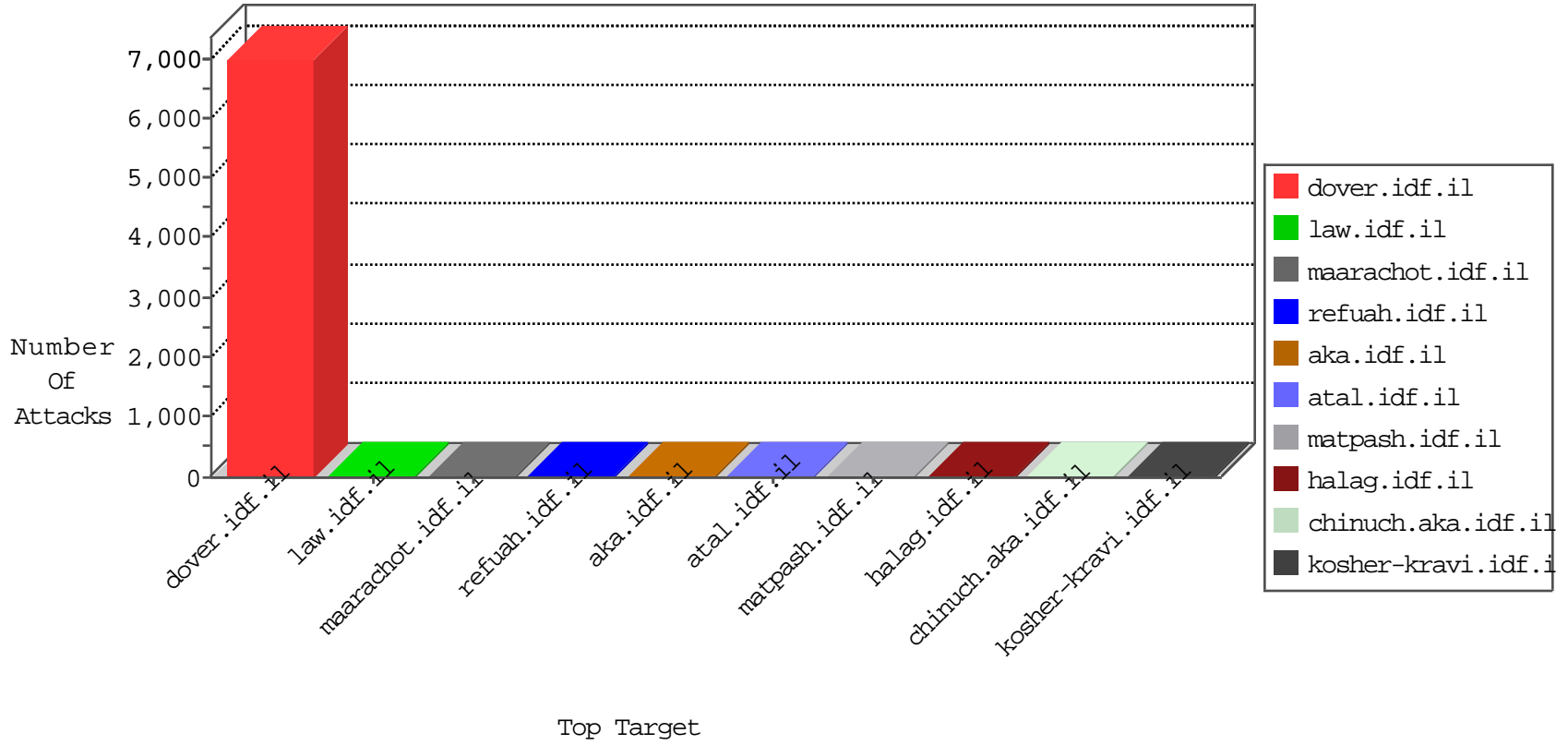


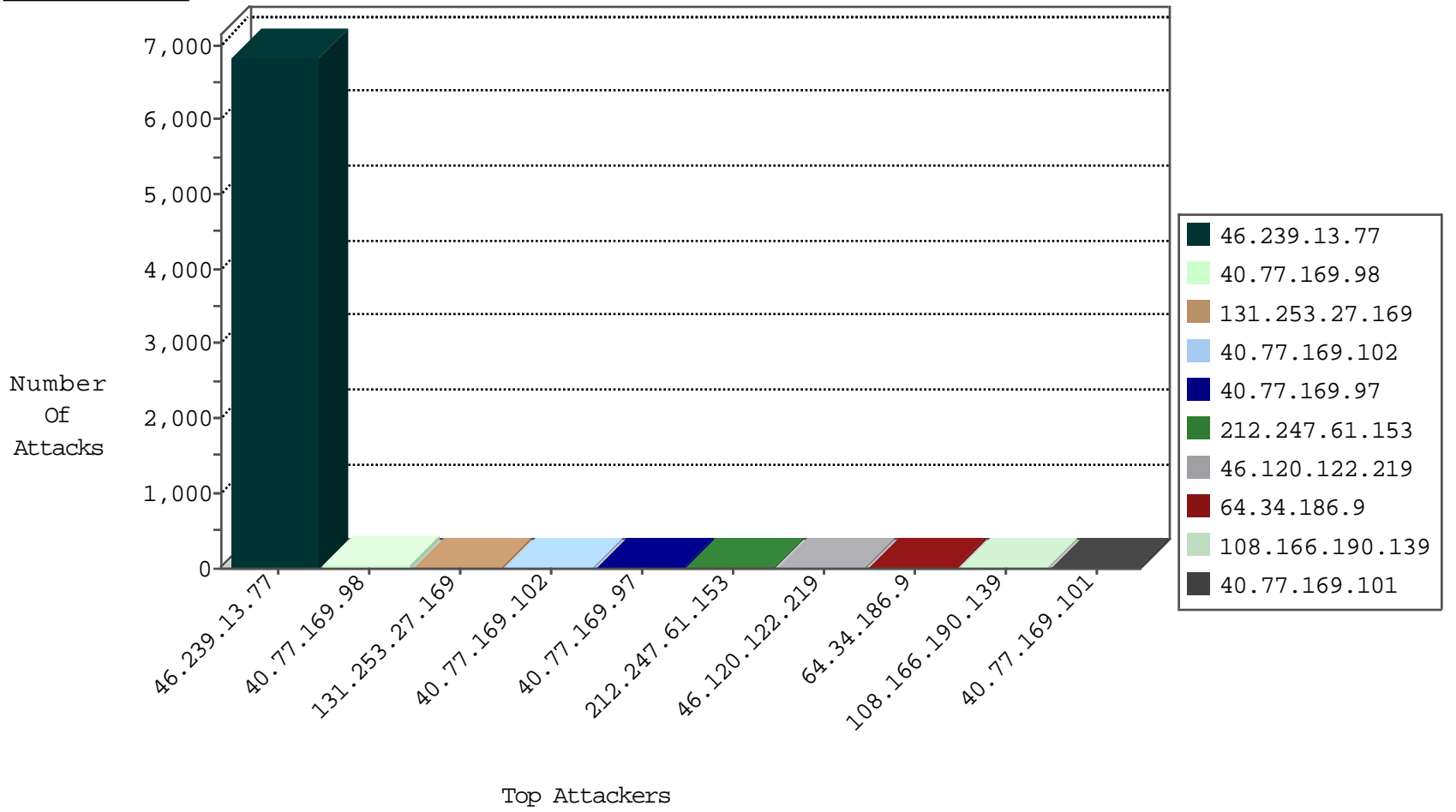
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
14.152.81.71	China	147.237.76.147	chinuch.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
134.147.203.115	Germany	147.237.76.147	chinuch.aka.idf.il	Black List	drop	2
104.148.35.34	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
64.34.186.9	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
108.166.190.139	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
51.255.48.155	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	16
64.34.186.9	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
108.166.190.139	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
91.201.236.50	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 3072	1
149.56.25.226	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.172	147.237.76.39	Sweden	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
173.81.79.48	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.13.77	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6695
46.239.13.77	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	150
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
212.247.61.153	Sweden	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	18
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
40.77.169.98	United States	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	8
87.117.203.23	United Kingdom	147.237.77.233	atal.idf.il	drop	SAM rule	drop	6
40.77.169.98	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	4
40.77.169.100	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
40.77.169.99	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
176.13.250.133	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
40.77.169.100	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.0.200	m4u.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.44	e.refuah.idf.il	drop	SAM rule	drop	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.227	e.hamaz.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.8.27	e.madim.atal.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.72.217	e.idf.il	drop	SAM rule	drop	1
46.19.86.25	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.201	e.atal.idf.il	drop	SAM rule	drop	1
158.130.6.191	United States	147.237.0.33	idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
131.253.27.169	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	24
199.30.24.217	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
40.77.169.96	United States	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in URL from 40.77.169.96	Block	2
199.30.24.115	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
40.77.169.96	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 40.77.169.96	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
121.199.7.98	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
2.50.178.103	United Arab Emirates	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/wp-login.php	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
2.50.178.103	United Arab Emirates	147.237.0.15	kosher-kravi.idf.il	Distributed PHP Attempt	Block	1
67.175.18.68	United States	147.237.77.216	dover.idf.il	NULL Character in Method i[[#0]][[#0]][[#0]]B6YÄÜm[[#18]]*k&b=æ[[#19]][[#15]]í[[#27]]S•Ä[[#3]][[#5]][[#6]]¶Á[[#11]]Mwİl"%[[#20]]TAF.ZLİ[[#5]]É!*k>M">°ä[[#26]]üÜøÚ{ô:h%örP+[[#20]]Y,ùÈoöf4æ^%Hßø.Pr%[[#4]]ÖÜläg{H{•}()	Block	1
65.55.210.93	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
158.130.6.191	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/images/	Block	1
2.50.178.103	United Arab Emirates	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/wp-login.php	Block	1
121.199.7.98	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 121.199.7.98	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
2.50.176.9	United Arab Emirates	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
199.30.24.253	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
121.199.7.98	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 121.199.7.98	Block	1
2.50.178.103	United Arab Emirates	147.237.77.234	halag.idf.il	Distributed PHP Attempt	Block	1
2.50.178.103	United Arab Emirates	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 2.50.178.103	Block	1
84.229.67.163	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
67.175.18.68	United States	147.237.77.216	dover.idf.il	Unknown HTTP Request Method i[[#0]][[#0]][[#0]]B6YÄÜm[[#18]]*k&b=æ[[#19]][[#15]]í[[#27]]S•Ä[[#3]][[#5]][[#6]]¶Á[[#11]]Mwİl"%[[#20]]TAF.ZLİ[[#5]]É!*k>M">°ä[[#26]]üÜøÚ{ô:h%örP+[[#20]]Y,ùÈoöf4æ^%Hßø.Pr%[[#4]]ÖÜläg{H{•}() in URL	Block	1
65.55.210.240	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
180.76.15.27	China	147.237.0.19	madim.atal.idf.il	Parameter Type Violation returnUrl in madim.atal.idf.il/login.aspx	Block	1
2.50.178.103	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
121.199.7.98	China	147.237.77.74	law.idf.il	PHP Attempt	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
2.50.176.9	United Arab Emirates	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/wp-login.php	Block	1
66.249.76.116	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	1
2.50.178.103	United Arab Emirates	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 2.50.178.103	Block	1
2.50.178.103	United Arab Emirates	147.237.0.19	madim.atal.idf.il	Distributed PHP Attempt	Block	1
94.124.5.10	Poland	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
84.94.89.120	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
66.249.64.219	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
198.20.87.98	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
121.199.7.98	China	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
2.50.178.103	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
2.50.176.9	United Arab Emirates	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
67.175.18.68	United States	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
2.50.178.103	United Arab Emirates	147.237.0.19	madim.atal.idf.il	Multiple Unauthorized URL Access from 2.50.178.103	Block	1
109.64.151.180	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.65.12	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1893	Block	1
121.199.7.98	China	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
2.50.178.103	United Arab Emirates	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
84.95.208.20	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1