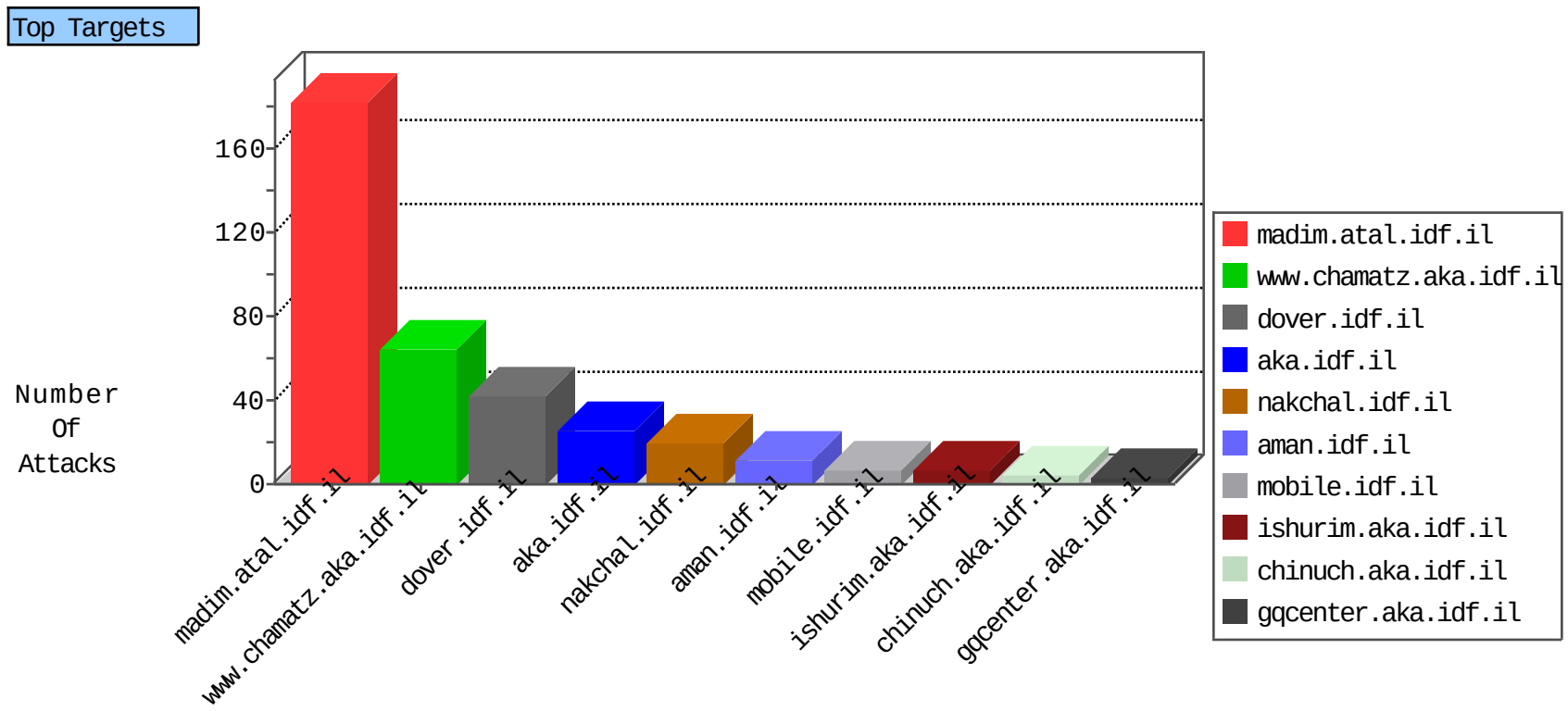
09-02-2016-10:04:08 to 09-02-2016-11:04:08

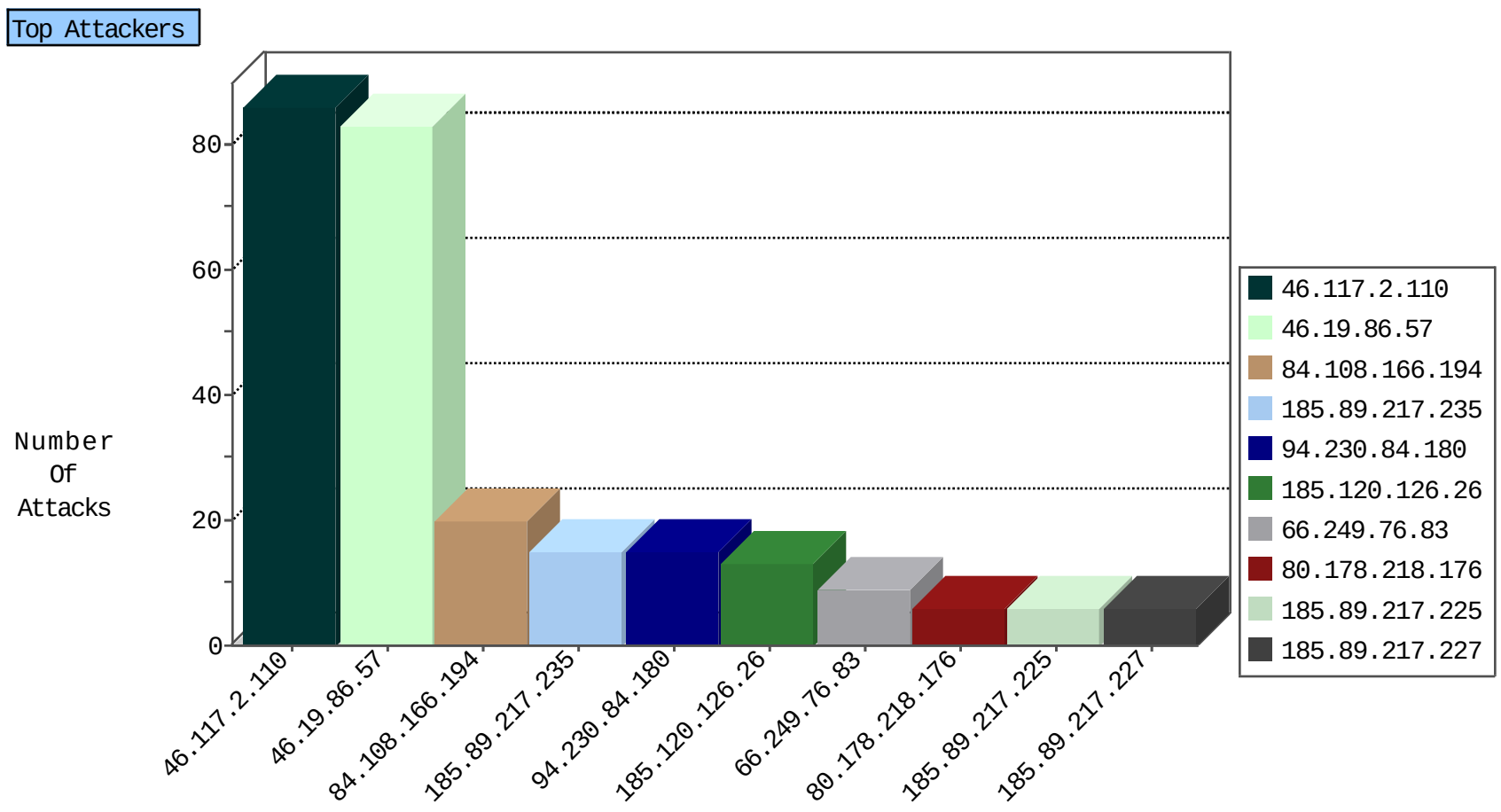
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-02-2016-10:04:08 to 09-02-2016-11:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.2	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	2
93.115.28.125	Romania	147.237.76.176	test.ncore.idf.il	Black List	drop	1
93.115.28.125	Romania	147.237.76.177	ncore.idf.il	Black List	drop	1
185.89.217.234	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	TCP handshake violation, first packet not syn	drop	1
5.233.249.192	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-02-2016-10:04:08 to 09-02-2016-11:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-02-2016-10:04:08 to 09-02-2016-11:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
59.46.193.114	147.237.72.156	China	aman.idf.il	GPL SCAN nmap TCP	2
218.24.171.223	147.237.72.156	China	aman.idf.il	GPL SCAN nmap TCP	2
62.210.124.129	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
93.174.93.220	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
186.170.127.182	147.237.0.35	Colombia	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.67.159.197	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	1
46.227.67.172	147.237.76.147	Sweden	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
192.223.90.236	147.237.76.44	Bolivia	e.refuah.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
163.172.169.150	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

09-02-2016-10:04:08 to 09-02-2016-11:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.89.217.235	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	15
185.120.126.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
185.89.217.228	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.233	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.225	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
80.178.218.176	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.227	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	6
185.89.217.229	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.234	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.230	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.226	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.231	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
185.89.217.232	Netherlands	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.178.46.178	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	3
82.81.17.144	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	1
31.13.113.64	Ireland	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
104.148.120.134	United States	147.237.0.35	akaws.idf.il	drop		drop	1
216.218.206.110	United States	147.237.0.200	m4u.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.199	e.nakchal.idf.il	drop	First packet isn't SYN	drop	1
104.148.120.134	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
216.218.206.118	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.200	m4u.idf.il	drop	First packet isn't SYN	drop	1
176.13.236.3	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
5.233.249.192	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.247.133	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.2.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
46.19.86.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
84.108.166.194	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	10
84.108.166.194	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/4/	Block	10
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	5
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
79.179.210.180	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/1088-he/meretz.aspx	Block	4
46.19.85.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.117.17.41	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.117.17.41	Block	3
213.151.37.161	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.53.17.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.46.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.79.122	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/apple-app-site-association	Block	1
213.151.39.226	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
94.230.84.180	Israel	147.237.77.216	dover.idf.il	NULL Character in Method ±BõgQ=ÊG•f[[#0]][[#19]]àÜØ-¹\=¦«>—•íg[[#25]]!Œ££i×[[#23]]p[[#25]]¬Œ‹¡šñ[[#4]]âÛ6œ[[#25]]Ã+»zi&È	Block	1
46.121.157.93	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
94.230.84.180	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name ,[[#28]]é[[#6]]²\L‘<k§à+ô¨‡I¾¬¯À½áeÒð«îGQJ¼Uþcy[[#3]]0÷[[#27]]EF[[#2]]q»ö Á™-[[#15]]„T2GÌòf!ü[[#4]]M0÷C¶J[[#5]]«[[#2]][[#0]]•ÏMù¾QûÑéÏàÌ'ÂB"zÅÉ¥[[#4]]Š„2¬c•ˆ¸[[#1]]Â¡$4ap«l\+h	Block	1
5.102.218.9	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.178.46.178	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1748	Block	1
128.232.110.28	United Kingdom	147.237.72.156	aman.idf.il	Unauthorized Method HEAD for 147.237.72.156/	Block	1
46.19.86.128	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
94.230.84.180	Israel	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 23	Block	1
2.53.149.189	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
66.249.88.154	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
94.230.84.180	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.121.157.93	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-login.php	Block	1
94.230.84.180	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Value	Block	1
37.26.147.158	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.179.210.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
141.226.162.133	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
94.230.84.180	Israel	147.237.77.216	dover.idf.il	Malformed URL תחה/fu6)‏ [[#5]]£ב–q."|ÿ~-!tm[[#31]]gž	Block	1
2.53.153.101	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
94.230.84.180	Israel	147.237.77.216	dover.idf.il	Too Many Headers per Request - 29 Headers	Block	1
66.249.66.100	Israel	147.237.0.15	kosher-kravi.idf.i	Distributed Unauthorized URL Access on kosher-kravi.idf.il/templates/departmentslobby/departmentslobby.aspx	Block	1
94.230.84.180	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method ±BõgQ=ÊG•f[[#0]][[#19]]àÜØ-¹\=¦«>—•íg[[#25]]!Œ££i×[[#23]]p[[#25]]¬Œ‹¡šñ[[#4]]âÛ6œ[[#25]]Ã+»zi&È	Block	1
79.179.210.180	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/login.aspx	Block	1
194.72.238.241	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1
94.230.84.180	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 94.230.84.180 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
94.230.84.180	Israel	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	Block	1
5.28.149.128	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
77.126.75.237	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	1
94.230.84.180	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method ±BõgQ=ÊG•f[[#0]][[#19]]àÜØ-¹\=¦«>—•íg[[#25]]!Œ££i×[[#23]]p[[#25]]¬Œ‹¡šñ[[#4]]âÛ6œ[[#25]]Ã+»zi&È	Block	1
66.249.66.102	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/templates/departmentslobby/departmentslobby.aspx	Block	1
46.19.85.239	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
94.230.84.180	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL תחה/fu6)‏ [[#5]]£ב–q."|ÿ~-!tm[[#31]]gž	Block	1
66.249.79.118	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
94.230.84.180	Israel	147.237.77.216	dover.idf.il	NULL Character in Header Name at }#0114Èàg[[#26]]=ÈÅ[[#15]],á[[[#6]]y‡=•WÑŠÍr="[[#21]]¡Ñ-[[#14]]o£]î„Ëò[[#3]]ÈVÁ*8ÛÜ[[#20]]=‰•¾¬×[[#22]]G[[#29]]ÒßhD«[[#5]]SÇ'¤g„[[#0]][[#27]]	Block	1
46.117.17.41	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1