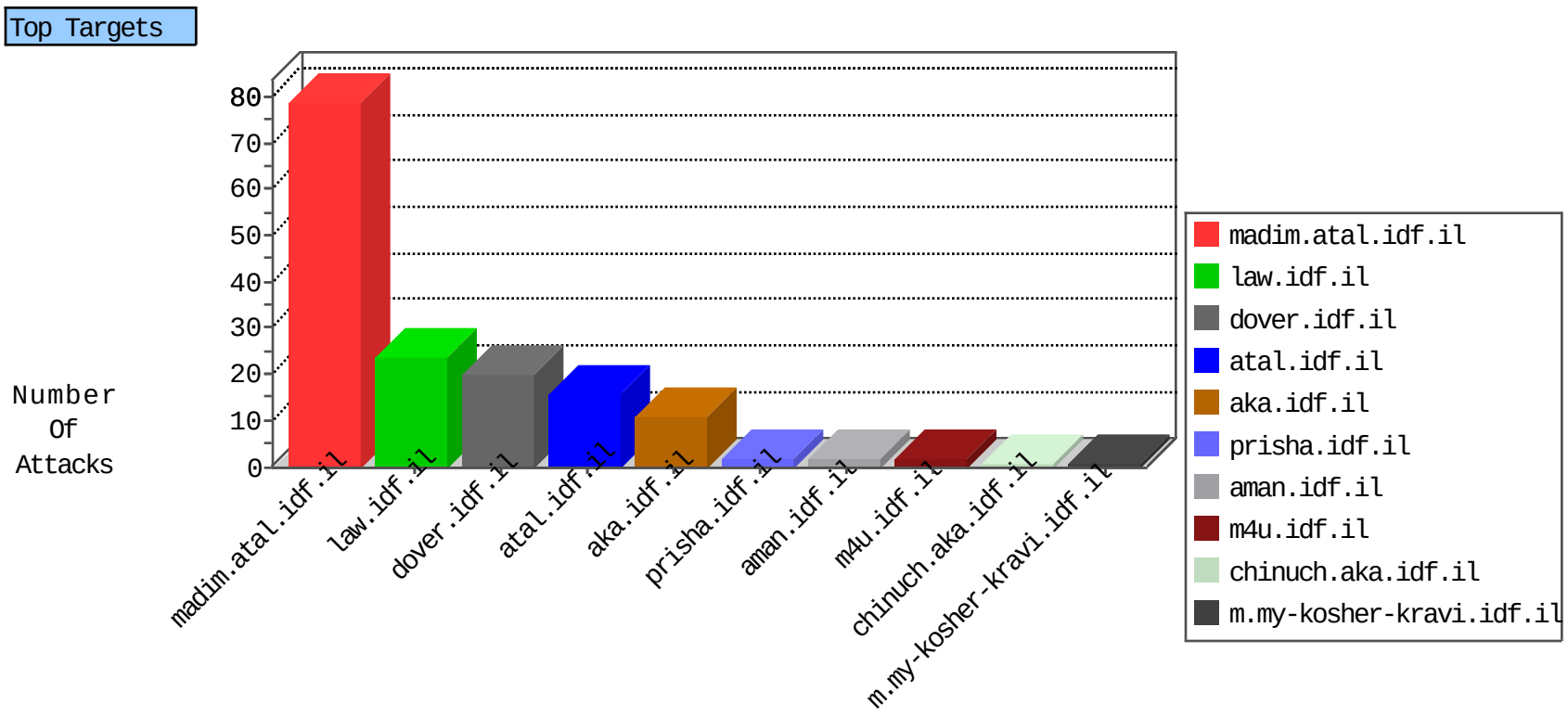
08-19-2016-09:04:01 to 08-19-2016-10:04:01

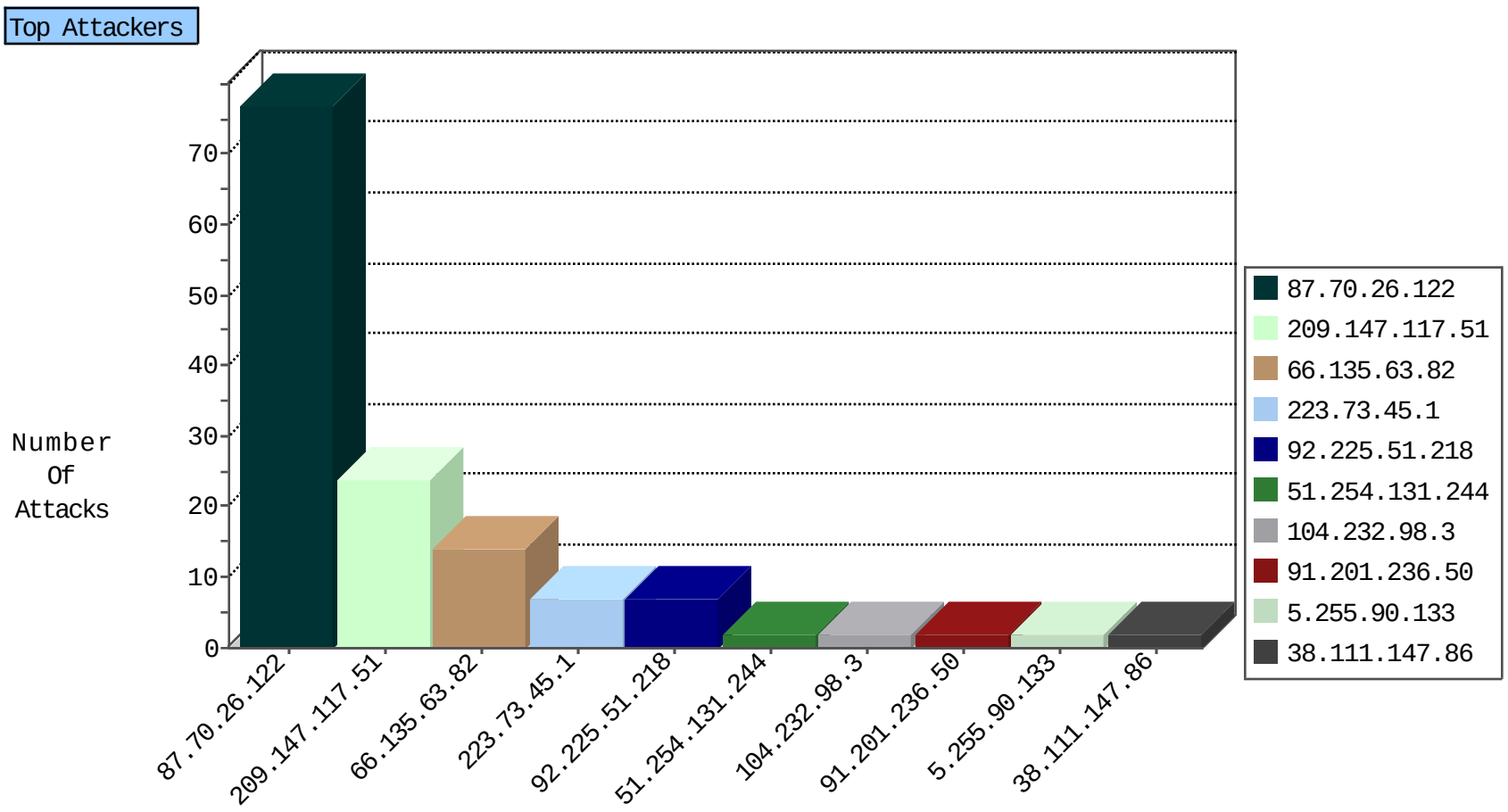
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-19-2016-09:04:01 to 08-19-2016-10:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-19-2016-09:04:01 to 08-19-2016-10:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.135.63.82	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
209.147.117.51	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
223.73.45.1	China	147.237.77.216	dover.idf.il	C1000125: HTTP: Block admin login to gov.il sites ?q=user	Permit	1
223.73.45.1	China	147.237.77.216	dover.idf.il	0872: HTTP: Apache .htaccess Access	Block	1
223.73.45.1	China	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Permit	1

08-19-2016-09:04:01 to 08-19-2016-10:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
209.147.117.51	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
66.135.63.82	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
5.255.90.133	147.237.76.38	Netherlands	e.e.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
185.40.195.206	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	ET SCAN NMAP -sA (2)	1
104.232.98.3	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
85.99.104.198	147.237.77.19	Turkey	law-forum.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.255.90.133	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.3	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
92.29.65.112	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN NMAP -sS window 1024	1

08-19-2016-09:04:01 to 08-19-2016-10:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
51.254.131.244	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
109.253.202.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
79.176.3.146	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.66.190.114	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1

08-19-2016-09:04:01 to 08-19-2016-10:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.70.26.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
92.225.51.218	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/megurim/	Block	5
223.73.45.1	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
109.253.244.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
92.225.51.218	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/social/undefined	Block	2
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.183	Block	1
109.66.35.4	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
77.138.35.136	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
50.161.67.238	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/olim	Block	1
66.249.69.245	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/general.aspx	Block	1
77.139.231.190	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
66.249.64.149	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/894-he	Block	1
223.73.45.1	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.76.122	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
203.127.96.245	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
80.246.140.132	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.64.155	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/news/news.aspx	Block	1
94.64.102.18	Greece	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.93.102	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
221.199.215.231	Australia	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
85.65.19.140	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.64.171	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/templates/news/news.aspx	Block	1
104.128.144.131	Canada	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/redirect.php	Block	1
68.180.228.227	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
223.73.45.1	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 223.73.45.1	Block	1

08-19-2016-09:04:01 to 08-19-2016-10:04:01