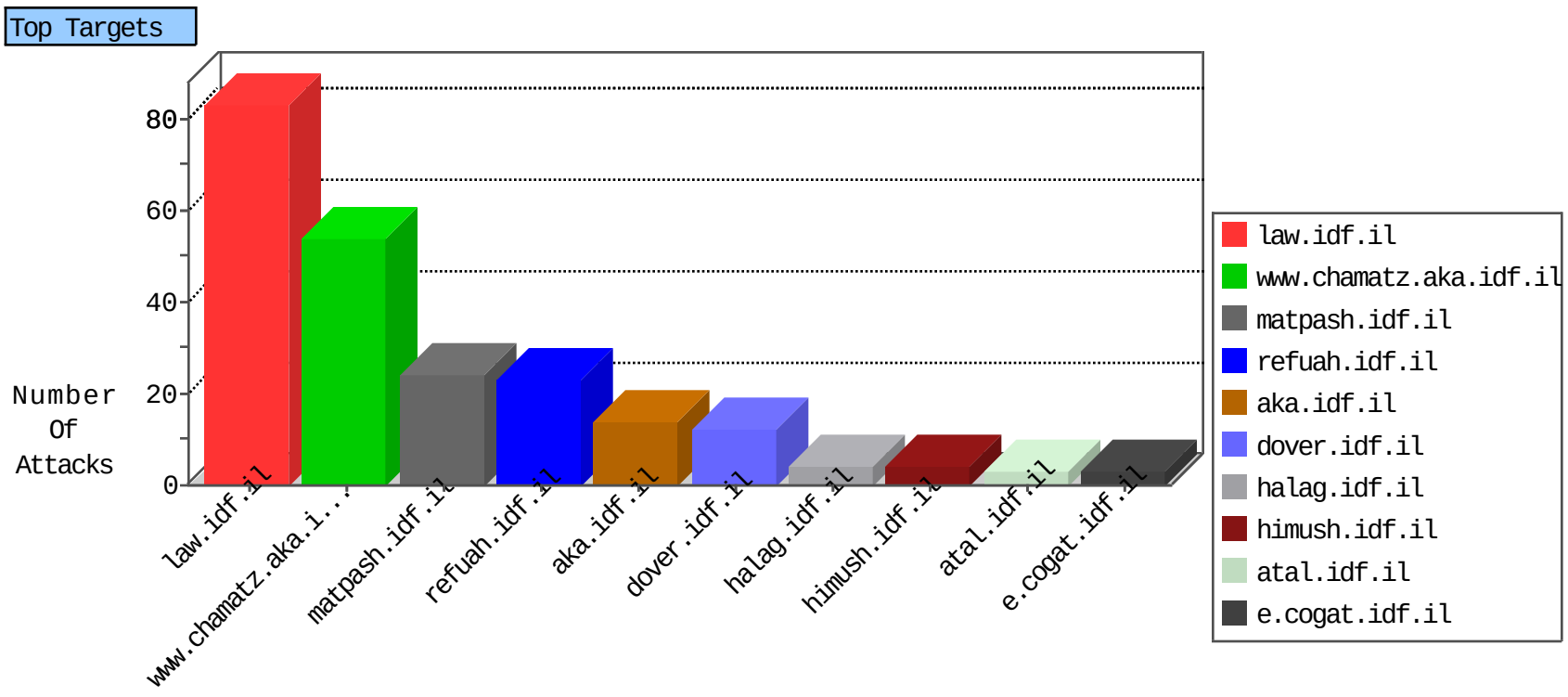
09-03-2016-05:04:01 to 09-03-2016-06:04:01

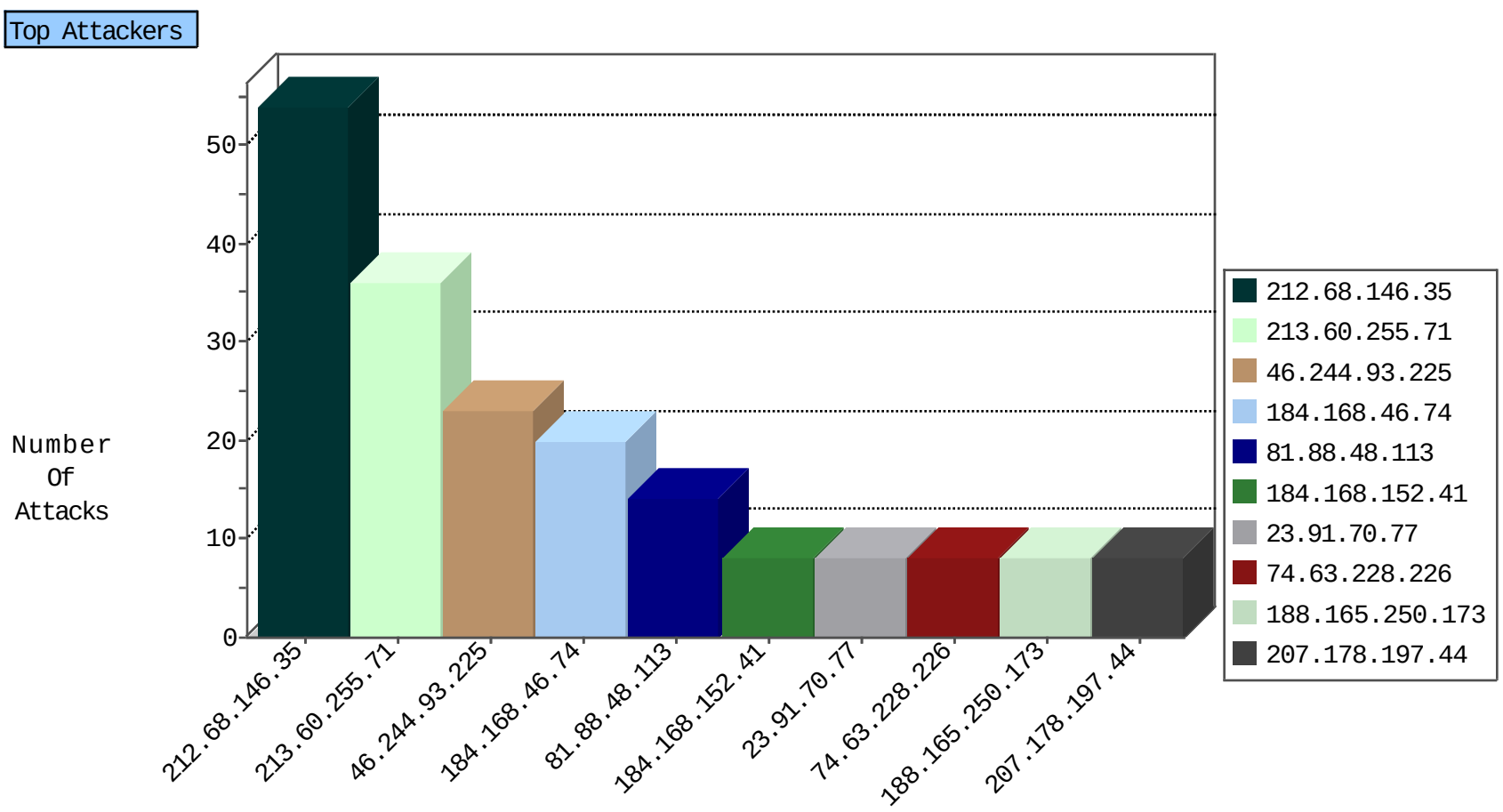
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-03-2016-05:04:01 to 09-03-2016-06:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
118.193.26.34	Hong Kong	147.237.76.30	himush.idf.il	Black List	drop	1
118.193.26.39	Hong Kong	147.237.76.30	himush.idf.il	Black List	drop	1
204.42.253.132	United States	147.237.76.86	navy.idf.il	Black List	drop	1

09-03-2016-05:04:01 to 09-03-2016-06:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-03-2016-05:04:01 to 09-03-2016-06:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.68.146.35	147.237.77.226	Israel	www.chamatz.aka.idf.il	SQL Injection - Select From	54
213.60.255.71	147.237.77.74	Spain	law.idf.il	SQL Injection - Select From	36
184.168.46.74	147.237.76.42	United States	refuah.idf.il	SQL Injection - Select From	20
81.88.48.113	147.237.77.74	Italy	law.idf.il	SQL Injection - Select From	14
207.178.197.44	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
184.168.152.41	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
74.63.228.226	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
188.165.250.173	147.237.77.74	France	law.idf.il	SQL Injection - Select From	8
23.91.70.77	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	8
80.246.130.158	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
221.204.249.157	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
123.176.80.201	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
208.100.26.228	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.155	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -f -sS	1
87.236.194.161	147.237.76.42	Czech Republic	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.106.200	147.237.0.15	India	kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
163.172.238.46	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.67.13	147.237.76.148	United Kingdom	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
123.176.80.201	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
217.165.67.151	147.237.0.34	United Arab Emirates	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
104.232.98.38	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
104.232.98.38	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
208.100.26.228	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.155	147.237.77.234	Ukraine	halag.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
83.84.137.88	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.106.200	147.237.0.15	India	kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
163.172.67.13	147.237.77.74	United Kingdom	law.idf.il	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN Potential SSH Scan	1

09-03-2016-05:04:01 to 09-03-2016-06:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.244.93.225	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	23
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
74.82.47.36	United States	147.237.0.35	akaws.idf.il	drop		drop	1
202.3.76.56		147.237.0.35	akaws.idf.il	drop		drop	1
119.81.249.132	Hong Kong	147.237.0.200	m4u.idf.il	drop		drop	1
52.28.32.164	Germany	147.237.76.34	yohalan.idf.il	drop		drop	1
183.129.160.229	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
52.28.32.164	Germany	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
183.129.160.229	China	147.237.72.217	e.idf.il	drop	SAM rule	drop	1
66.249.66.157	Israel	147.237.0.33	idf.il	drop		drop	1
184.105.247.211	United States	147.237.0.200	m4u.idf.il	drop		drop	1

09-03-2016-05:04:01 to 09-03-2016-06:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
131.253.25.196	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
86.135.150.254	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	2
207.46.13.90	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
40.77.167.8	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.66.222	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/templates/searchresultsidf/searchresultsidf.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.77	Block	1
46.19.86.237	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.14	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/smalim.aspx	None	1
66.249.75.43	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
198.20.69.74	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
66.249.75.101	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/navmenu/	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/69681.pdf	Block	1
207.46.13.77	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19178-he/dover	Block	1
66.249.76.8	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1119-he/אגף הטכנולוגיה והלוגיס aspx.טיקה	Block	1
66.249.64.245	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	Block	1

09-03-2016-05:04:01 to 09-03-2016-06:04:01