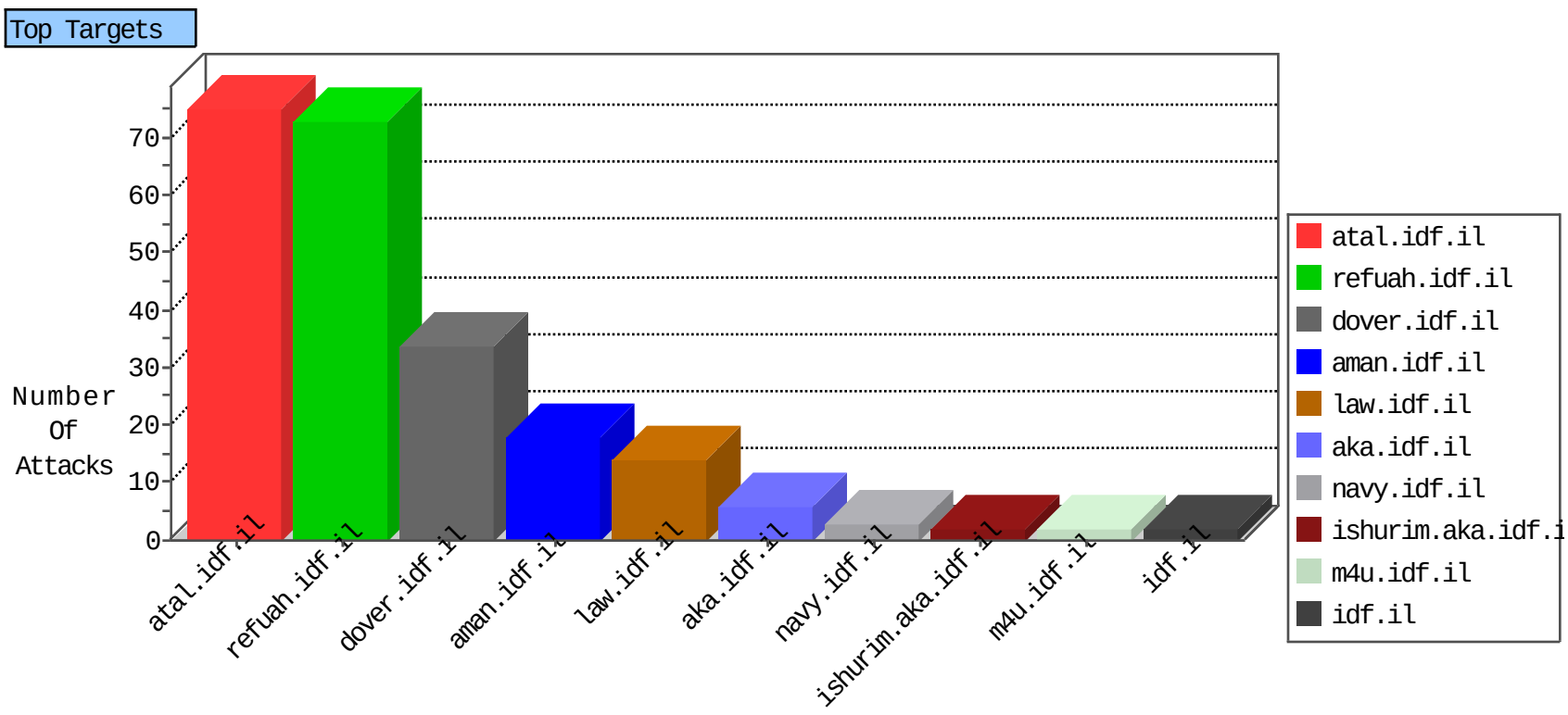
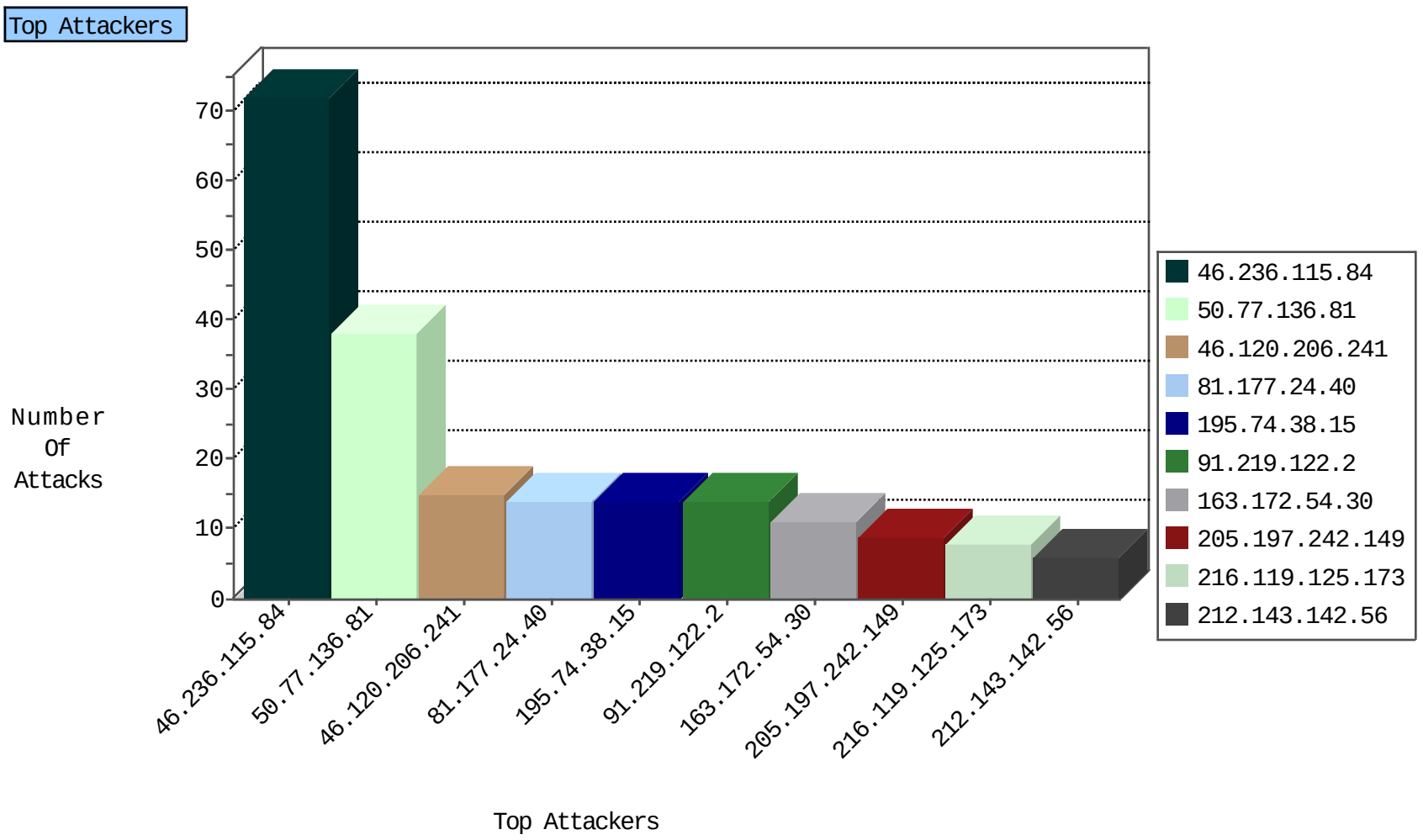
08-19-2016-03:04:02 to 08-19-2016-04:04:02

IDF Under Attack
Daily Report

Top Targets



Top Attackers



08-19-2016-03:04:02 to 08-19-2016-04:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.169.18	Israel	147.237.72.167	ishurim.aka.idf.il	Black List	drop	1
195.154.172.204	France	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1

08-19-2016-03:04:02 to 08-19-2016-04:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.236.115.84	Sweden	147.237.76.42	refuah.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
50.77.136.81	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
46.236.115.84	Sweden	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
81.177.24.40	Russian Federation	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
91.219.122.2	Poland	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.77.136.81	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
50.77.136.81	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
195.74.38.15	Sweden	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
216.119.125.173	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
199.58.86.206	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
195.74.38.15	Sweden	147.237.77.233	atal.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

08-19-2016-03:04:02 to 08-19-2016-04:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.236.115.84	147.237.76.42	Sweden	refuah.idf.il	SQL Injection - Select From	54
50.77.136.81	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	20
195.74.38.15	147.237.77.233	Sweden	atal.idf.il	SQL Injection - Select From	8
91.219.122.2	147.237.77.233	Poland	atal.idf.il	SQL Injection - Select From	8
81.177.24.40	147.237.77.74	Russian Federation	law.idf.il	SQL Injection - Select From	8
216.119.125.173	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	4
163.172.54.30	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.251	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
157.122.97.182	147.237.76.42	China	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.54.30	147.237.77.235	United Kingdom	sviva.idf.il	ET SCAN Potential SSH Scan	1
66.249.76.52	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
163.172.54.30	147.237.77.205	United Kingdom	prisha.idf.il	ET SCAN Potential SSH Scan	1
66.151.255.234	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.54.30	147.237.76.86	United Kingdom	navy.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
163.172.54.30	147.237.8.45	United Kingdom	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
163.172.54.30	147.237.0.33	United Kingdom	idf.il	ET SCAN Potential SSH Scan	1
163.172.54.30	147.237.0.17	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
95.86.73.225	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
94.102.48.195	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
185.118.65.230	147.237.8.24	Russian Federation	e.lifestyle.idf.il	ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack	1
163.172.54.30	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN Potential SSH Scan	1
66.249.65.129	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
163.172.54.30	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
163.172.54.30	147.237.76.39	United Kingdom	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
163.172.54.30	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN Potential SSH Scan	1

08-19-2016-03:04:02 to 08-19-2016-04:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.120.206.241	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
205.197.242.149	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
157.55.39.110	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
31.13.102.106	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
38.111.147.86	United States	147.237.77.216	dover.idf.il	drop		drop	2
169.229.3.91	United States	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
31.13.112.122	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
31.13.102.126	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
31.13.110.110	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
212.143.165.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
139.162.37.113	United States	147.237.0.33	idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1
31.13.110.118	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-19-2016-03:04:02 to 08-19-2016-04:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
220.181.108.120	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/maslulim/rightarrowenabled.gif	Block	1
66.249.65.173	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/10012011yezu.aspx	Block	1
70.106.143.130	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
2.53.189.199	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
220.255.182.92	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.138.82.140	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/about.aspx	Block	1
66.249.65.133	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/general.aspx	Block	1
220.255.183.134	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.52	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.52	Block	1
84.111.110.197	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
66.249.65.166	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list1.htm	Block	1
220.255.219.58	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.52	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/apple-app-site-association	Block	1
203.127.96.246	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.65.172	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1

08-19-2016-03:04:02 to 08-19-2016-04:04:02