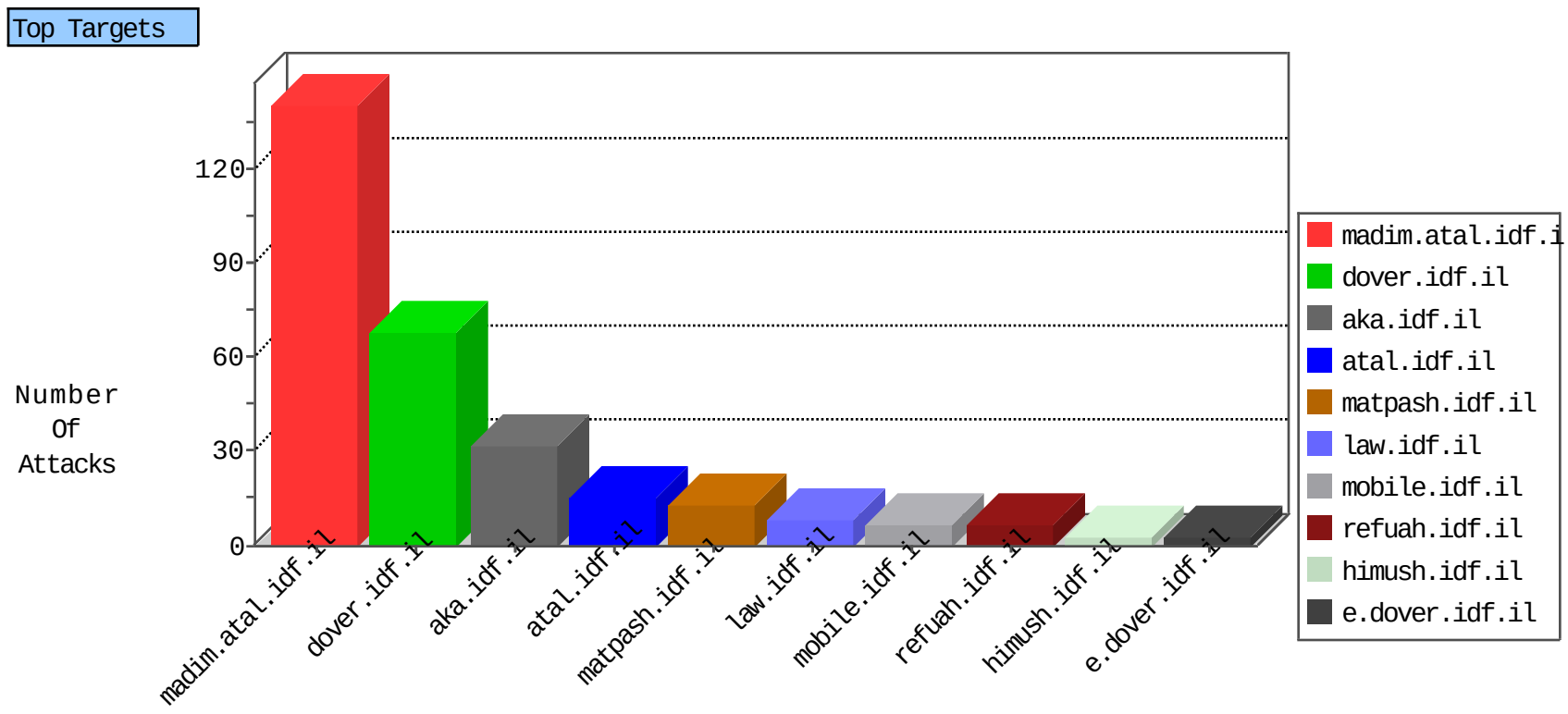
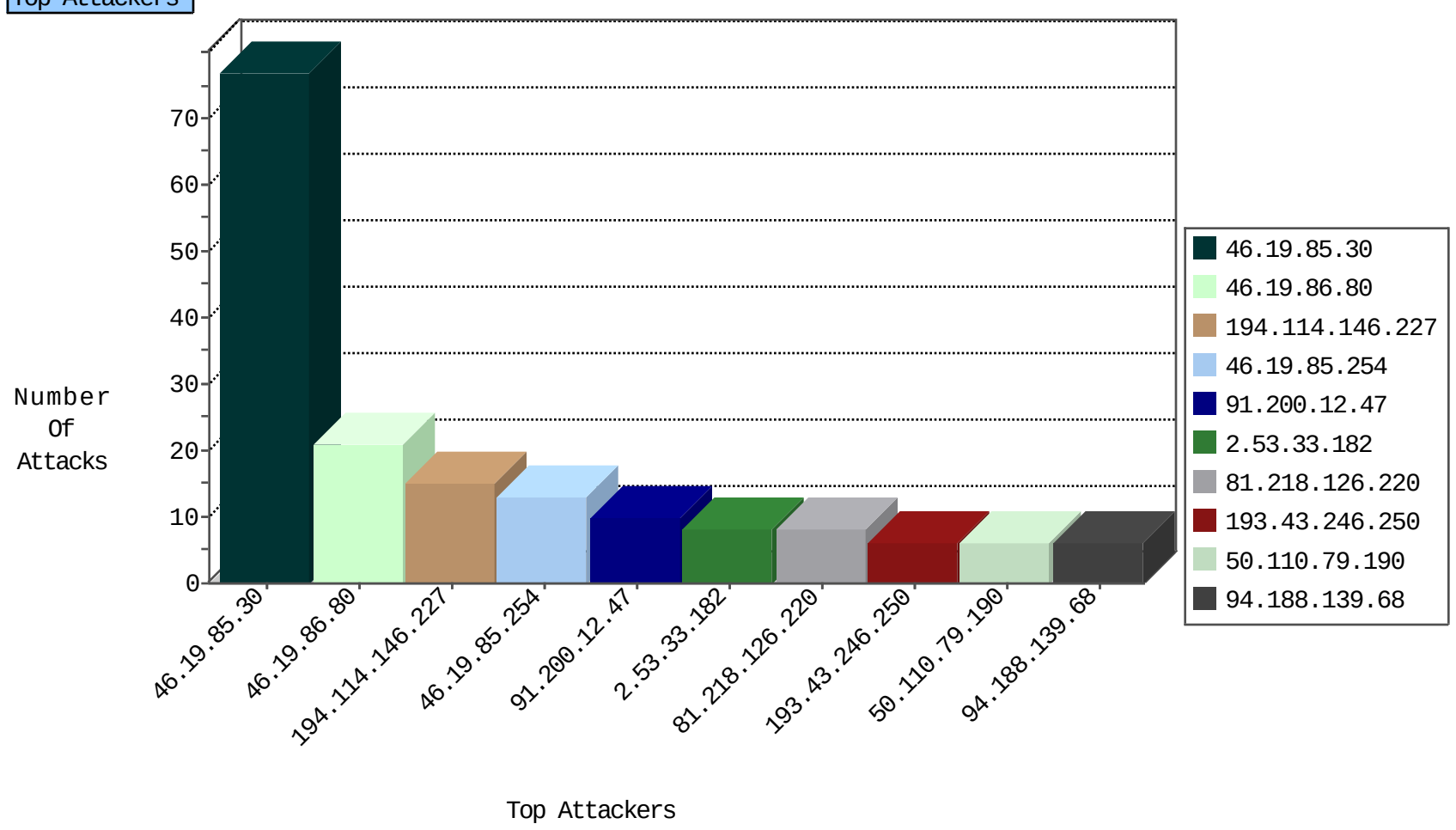
08-17-2016-09:04:09 to 08-17-2016-10:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



08-17-2016-09:04:09 to 08-17-2016-10:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.168.194.95	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
23.251.55.182	United States	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
80.82.69.221	Netherlands	147.237.76.30	himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
93.158.200.118	Netherlands	147.237.76.30	himush.idf.il	Black List	drop	1

08-17-2016-09:04:09 to 08-17-2016-10:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.200.12.47	Ukraine	147.237.77.233	atal.idf.il	C1000016: HTTP: administrator in URI	Permit	8
50.110.79.190	United States	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	3
50.110.79.190	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
50.110.79.190	United States	147.237.77.233	atal.idf.il	C1000074: HTTP: majestic bot	Permit	1

08-17-2016-09:04:09 to 08-17-2016-10:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
81.218.40.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.120.125.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
138.68.30.205	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.77.212	India	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
103.207.39.82	147.237.76.148	Vietnam	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
93.158.215.177	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
82.20.219.5	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.101.184.237	147.237.76.86	Germany	navy.idf.il	ET SCAN NMAP -sS window 1024	1
211.23.156.152	147.237.76.196	Taiwan	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
176.13.20.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
112.196.49.101	147.237.77.212	India	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
112.196.49.101	147.237.77.212	India	e.dover.idf.il	ET SCAN NMAP -f -sS	1
93.158.215.182	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
84.111.113.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

08-17-2016-09:04:09 to 08-17-2016-10:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.114.146.227	Israel	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	10
94.188.139.68	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.21.120.220	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
194.114.146.227	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
109.253.156.51	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
37.76.212.32	Palestinian Territory, Occupied	147.237.77.216	dover.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
176.13.3.234	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.120.124.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.139.118.215	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
95.35.74.19	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
109.253.218.105	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.247.208	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
137.116.71.170	United States	147.237.0.33	idf.il	drop		drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.137.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.20.194	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
109.253.157.214	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
176.13.241.255	Israel	147.237.77.243	mobile.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
46.19.85.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
46.19.86.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.19.85.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
2.53.33.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
109.253.207.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.55.147.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
81.218.126.220	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	4
46.19.86.99	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	4
131.253.25.156	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
81.218.126.220	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 81.218.126.220	Block	3
109.253.205.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.203	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
65.55.213.26	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
212.199.57.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	2
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
195.95.183.254	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1361-10650-he/dover.aspx.	Block	2
64.62.219.162	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
80.246.130.41	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
91.200.12.47	Ukraine	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/wp-login.php	Block	1
207.46.13.145	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1540-13036-he/dover.aspx target=	Block	1
81.218.40.194	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storag	Block	1
192.243.55.134	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
2.55.53.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.179.27.246	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
194.90.15.61	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/6/size338x0/1806.jpg	Block	1
192.243.55.129	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/chinuch/klali/default.asp?catid=60357&docid=	Block	1
46.121.128.215	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
109.66.59.24	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
192.243.55.137	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/tizmoret/gallery	Block	1
66.249.93.77	Israel	147.237.77.233	atal.idf.il	Distributed URL is Above Root Directory	Block	1
157.55.39.176	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
79.179.27.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/gallery	Block	1
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
212.179.229.115	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.93.111	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
192.243.55.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59268&docid=76123	Block	1
46.19.86.29	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
169.159.103.0	Nigeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
204.79.180.137	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/tmuna/?pictype=2&docid=33304	Block	1
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Malformed URL http/1.1	Block	1
81.218.126.220	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/7/	Block	1
77.139.23.128	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1