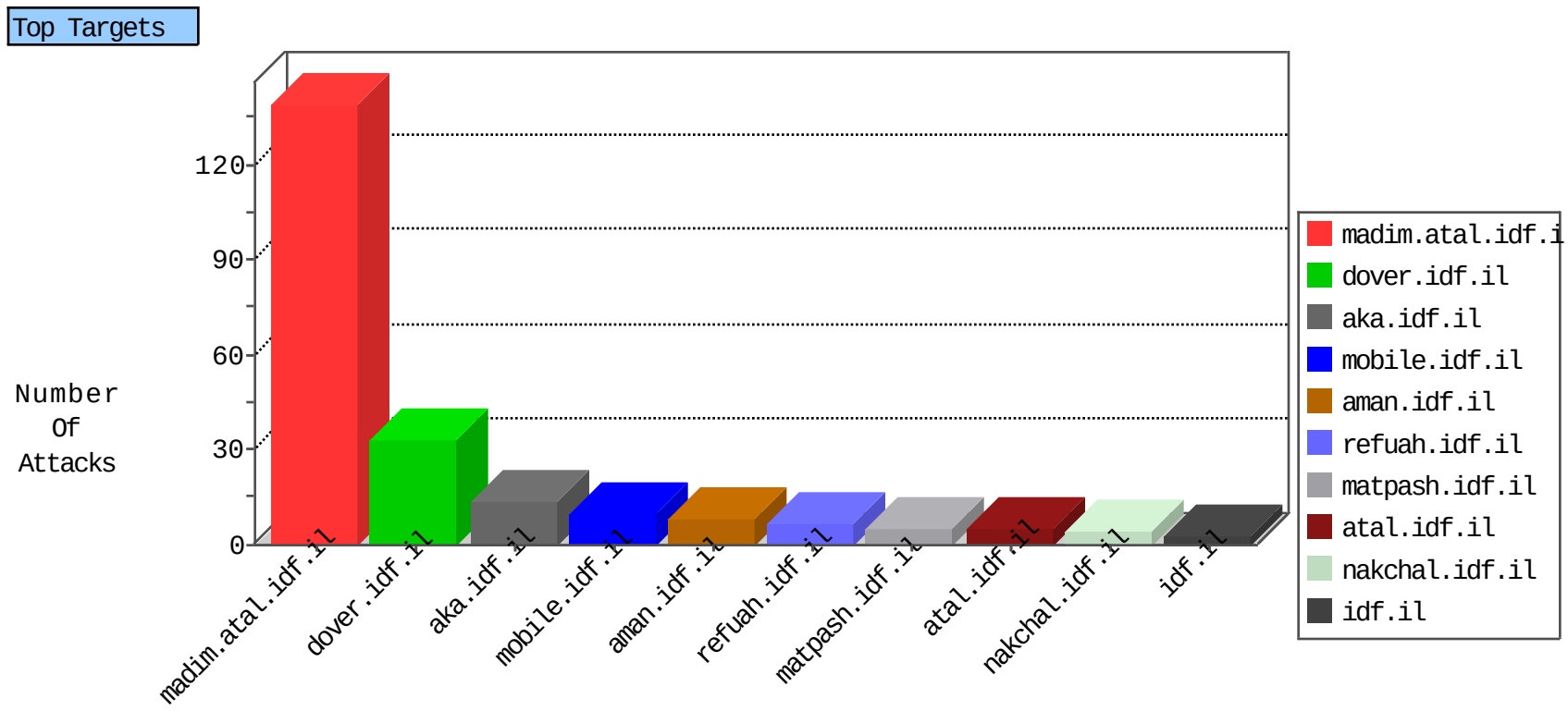
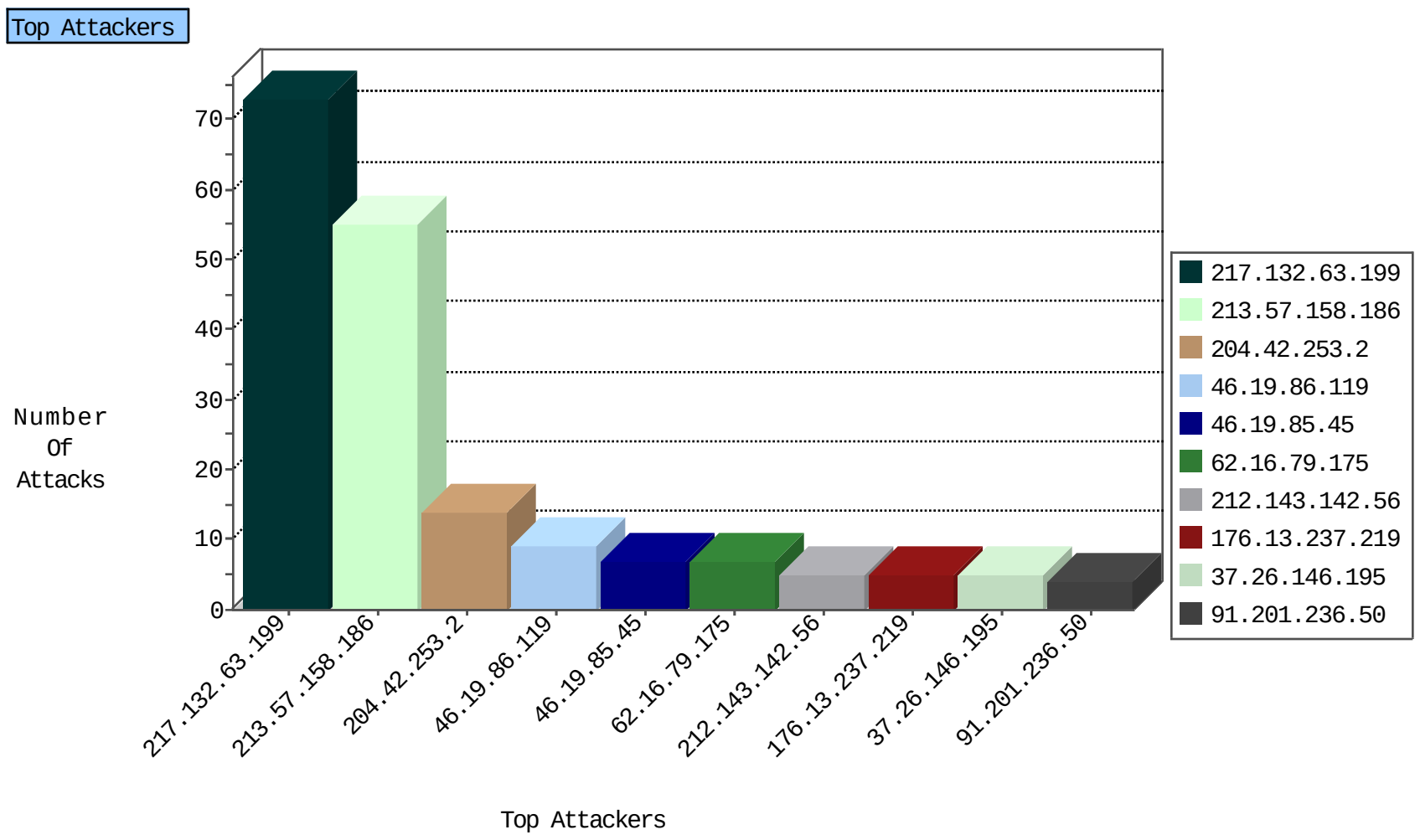
09-02-2016-13:04:01 to 09-02-2016-14:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-02-2016-13:04:01 to 09-02-2016-14:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.2	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.202	e.halag.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.197	e.himush.idf.il	Black List	drop	2
204.42.253.2	United States	147.237.76.201	e.atal.idf.il	Black List	drop	2
163.172.216.36	United Kingdom	147.237.76.44	e.refuah.idf.il	Black List	drop	1
91.230.107.174	Russian Federation	147.237.76.202	e.halag.idf.il	Black List	drop	1
141.212.122.164	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
141.212.122.165	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1

09-02-2016-13:04:01 to 09-02-2016-14:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-02-2016-13:04:01 to 09-02-2016-14:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.201.236.50	147.237.77.233	Ukraine	atal.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.77.233	Ukraine	atal.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.48.195	147.237.72.167	Netherlands	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.77.233	Ukraine	atal.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.50	147.237.77.233	Ukraine	atal.idf.il	ET SCAN NMAP -f -sS	1
5.255.90.133	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
168.235.197.231	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
104.232.98.38	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1

09-02-2016-13:04:01 to 09-02-2016-14:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.45	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
62.16.79.175	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
62.16.79.175	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
109.253.193.219	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
176.13.12.219	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
37.26.146.189	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
216.243.31.2	United States	147.237.0.33	idf.il	drop		drop	1
184.105.247.240	United States	147.237.0.33	idf.il	drop		drop	1
216.243.31.2	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
185.65.252.10	Iraq	147.237.76.34	yohalan.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
74.82.47.7	United States	147.237.0.33	idf.il	drop		drop	1
183.129.160.229	China	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
216.218.206.84	United States	147.237.0.35	akaws.idf.il	drop		drop	1
74.82.47.46	United States	147.237.0.200	m4u.idf.il	drop		drop	1
183.129.160.229	China	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1
46.119.127.129	Ukraine	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1

09-02-2016-13:04:01 to 09-02-2016-14:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.132.63.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	73
213.57.158.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
37.26.146.195	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	5
207.46.13.77	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.226.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.237.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.39.95	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.39.95	Block	2
176.13.20.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
131.253.25.232	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
131.253.27.168	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.129.239	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
46.19.86.25	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.76.9	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.in.aspx	Block	1
176.13.237.219	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1677	Block	1
131.253.25.150	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.127.19.196	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.24	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
87.69.39.95	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	1
66.249.76.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
176.228.163.67	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
77.138.249.140	France	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
213.151.47.80	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
66.102.9.118	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
104.148.120.134	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 104.148.120.134	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
185.27.105.131	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
131.253.27.84	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.139.254.99	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-9067-he/atal.aspx	Block	1
104.148.120.134	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to 147.237.76.147/user/login	Block	1
66.249.76.121	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/faq/faq.aspx	Block	1
46.19.86.6	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
188.186.76.62	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
79.177.160.156	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.14	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
176.13.237.219	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.237.219	Block	1

09-02-2016-13:04:01 to 09-02-2016-14:04:01