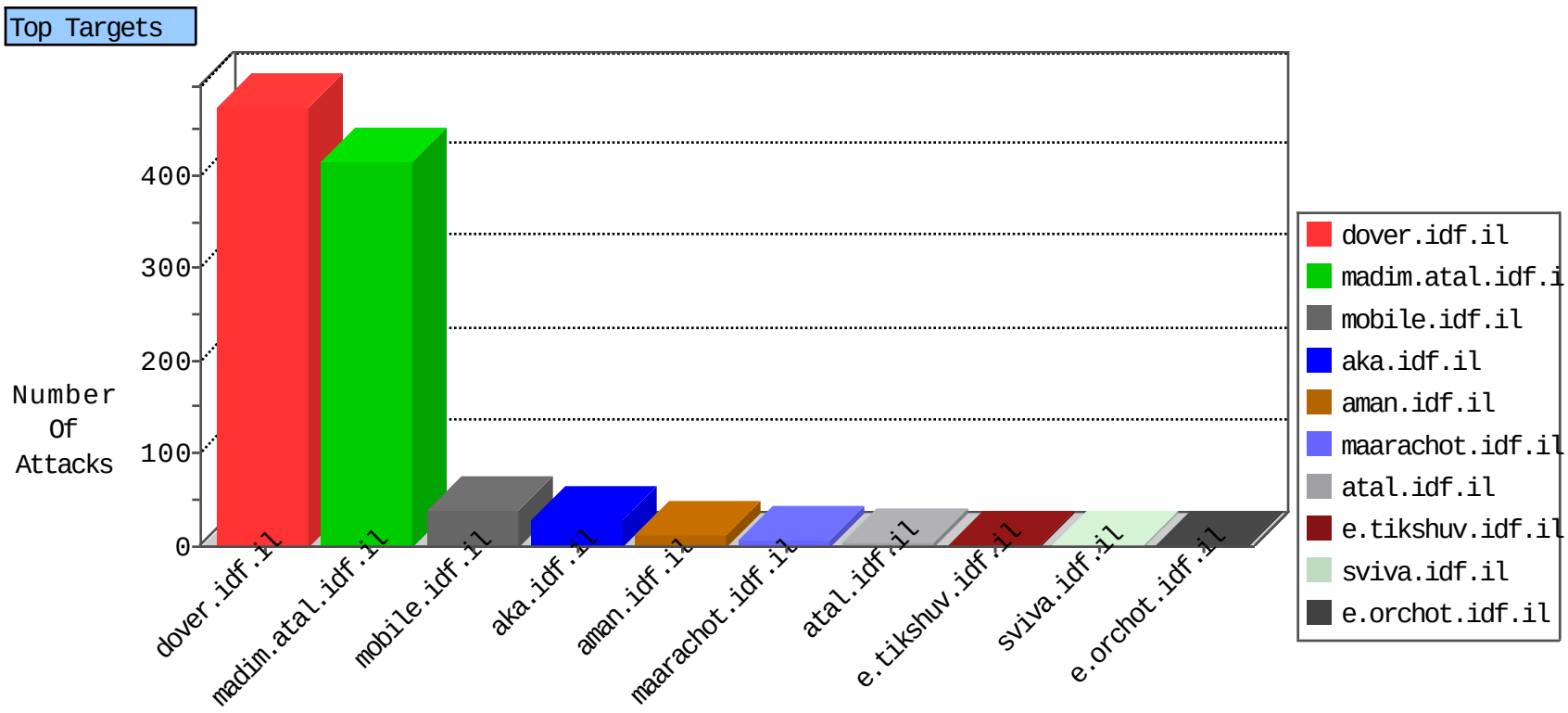
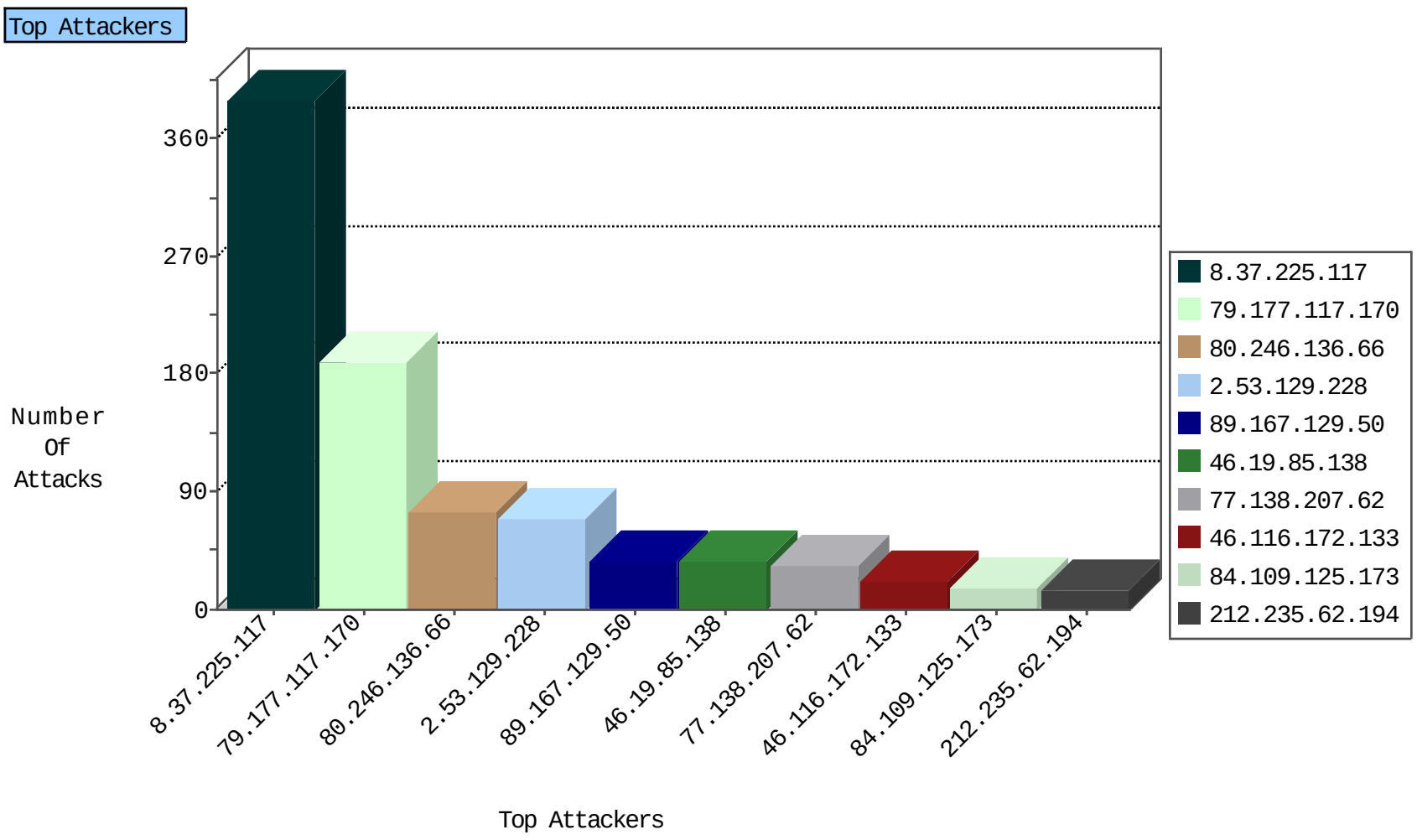
09-02-2016-17:04:04 to 09-02-2016-18:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-02-2016-17:04:04 to 09-02-2016-18:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.62.123	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
109.65.87.244	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
207.46.13.90	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
8.37.225.117	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
66.249.69.14	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
115.230.125.146	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
115.230.125.146	China	147.237.76.201	e.atal.idf.i	JLM_Under_Attack_Con_Tcp	drop	1

09-02-2016-17:04:04 to 09-02-2016-18:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-02-2016-17:04:04 to 09-02-2016-18:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
85.250.182.240	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	3
216.81.230.167	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
185.56.82.22	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
54.221.47.62	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
208.100.26.228	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.8.14	United Kingdom	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
85.65.199.38	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

09-02-2016-17:04:04 to 09-02-2016-18:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.225.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	387
89.167.129.50	Spain	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
84.109.125.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
89.167.129.50	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.67.211.89	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
176.13.21.146	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
89.167.129.50	Spain	147.237.77.216	dover.idf.il	drop		drop	5
41.227.134.113	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.179.49.139	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
109.253.139.220	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
156.205.199.204	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.247.218	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

09-02-2016-17:04:04 to 09-02-2016-18:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.117.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	189
80.246.136.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	75
2.53.129.228	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	69
46.19.85.138	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
77.138.207.62	France	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
212.235.62.194	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	15
46.116.172.133	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	13
46.116.172.133	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	9
89.167.129.50	Spain	147.237.77.216	dover.idf.il	Unauthorized Request Content Type from 89.167.129.50	Block	5
46.19.85.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.250.159.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.124.9.195	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
62.0.102.190	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	2
46.19.86.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.198.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.138.26.134	France	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
213.57.59.50	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
93.172.213.100	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ https:/twitter.com/	Block	1
79.178.33.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1815-he/dover.aspx	Block	1
62.0.102.190	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 62.0.102.190	Block	1
141.0.14.219	Europe	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim	Block	1
87.68.49.245	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.102.253.33	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
77.138.143.26	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	1
213.151.35.216	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniotanswer.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/18205.pdf	Block	1
109.64.97.84	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
79.183.58.221	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
148.251.179.145	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
87.70.243.55	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
40.77.167.29	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/1/63141.doc	Block	1
109.66.142.46	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1275-he/atal.aspx	Block	1
77.125.22.41	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
194.90.66.9	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
62.0.102.190	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/sip_storage/files/4/	Block	1
46.19.85.26	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.237.138.202	Czech Republic	147.237.77.235	sviva.idf.il	Unauthorized Method HEAD for /	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-ar/www.idf.il/ar	Block	1
109.66.166.22	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
84.94.67.206	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
2.53.132.71	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.127.0.156	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
93.172.213.100	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 93.172.213.100	Block	1
66.249.79.129	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
2.55.134.28	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1

09-02-2016-17:04:04 to 09-02-2016-18:04:04