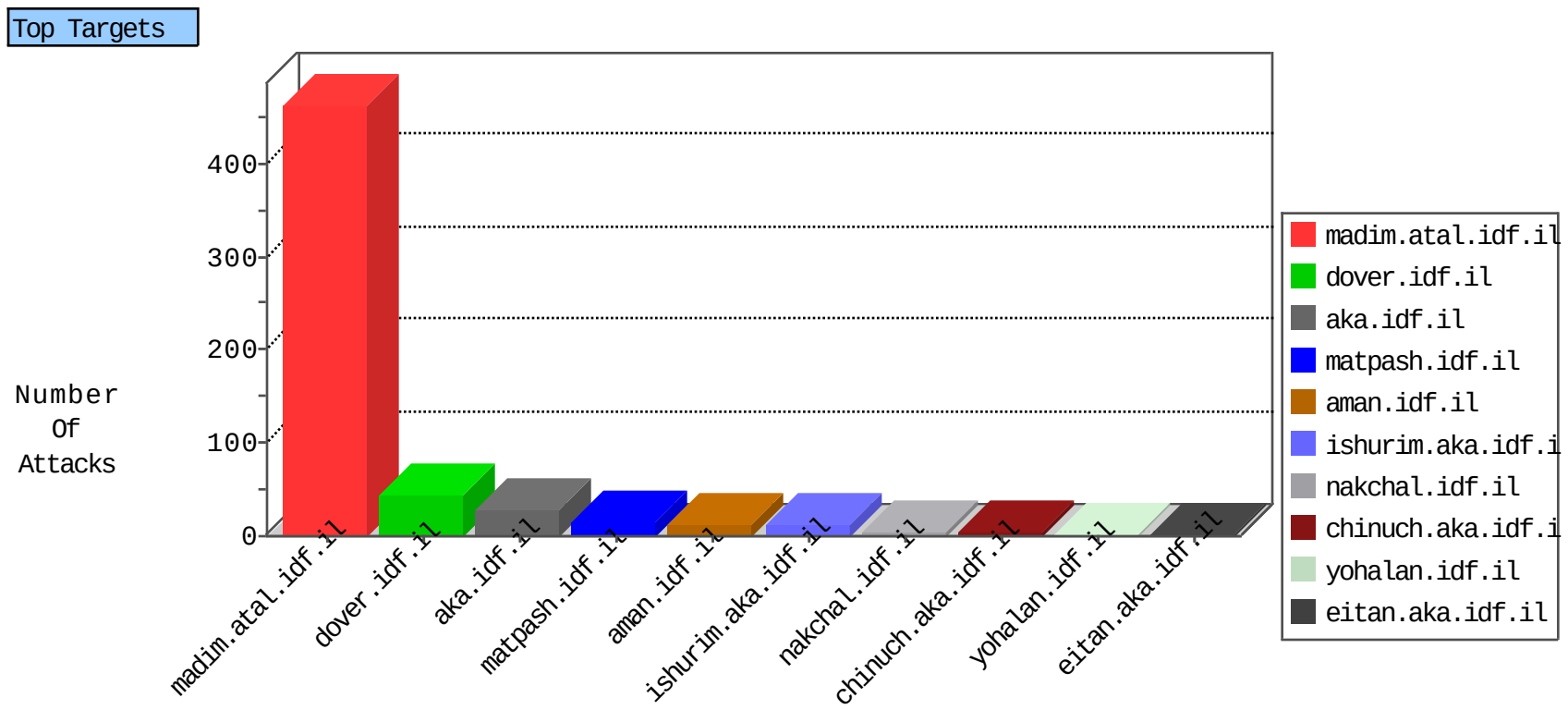
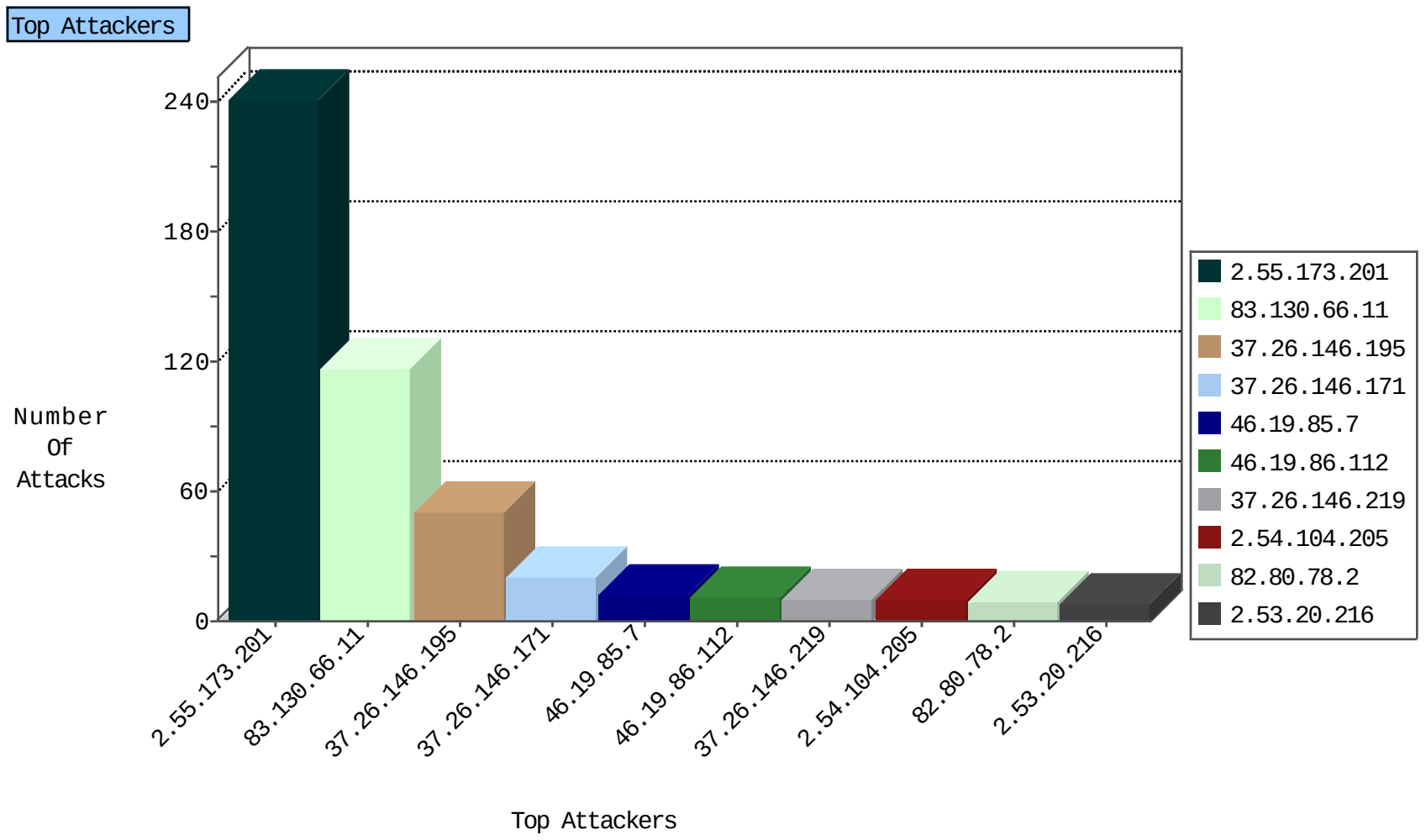
08-21-2016-20:04:08 to 08-21-2016-21:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-21-2016-20:04:08 to 08-21-2016-21:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
180.97.106.37	China	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
180.97.106.37	China	147.237.76.196	e.sviva.idf.il	Black List	drop	1
111.185.237.96	Taiwan	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
180.97.106.37	China	147.237.76.86	navy.idf.il	Black List	drop	1

08-21-2016-20:04:08 to 08-21-2016-21:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.165	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
164.132.161.86	Italy	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-21-2016-20:04:08 to 08-21-2016-21:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	4
52.32.89.208	147.237.77.216	United States	dover.idf.il	Xenu Link Sleuth User Agent	1

08-21-2016-20:04:08 to 08-21-2016-21:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.112	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	11
2.54.104.205	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
213.99.35.115	Spain	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
85.130.231.236	Israel	147.237.76.31	nakchal.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
188.227.239.66	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
176.13.248.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.223.6	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.33	idf.il	drop		drop	1
167.250.16.0	Brazil	147.237.0.35	akaws.idf.il	drop		drop	1
109.64.91.77	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
185.120.126.15	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.98	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
109.253.135.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.99	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
46.117.182.13	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.23.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.198.222	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.104	United States	147.237.0.200	m4u.idf.il	drop		drop	1
79.180.41.28	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.242.37	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
109.253.203.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.105	United States	147.237.0.200	m4u.idf.il	drop		drop	1

08-21-2016-20:04:08 to 08-21-2016-21:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.173.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	241
83.130.66.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	117
37.26.146.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
37.26.146.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
46.19.85.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
37.26.146.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
2.53.20.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
77.138.138.166	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	7
185.32.179.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
105.203.254.7	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
105.203.254.12	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
109.253.243.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
157.55.39.38	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
64.62.219.166	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
89.138.190.55	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 89.138.190.55 (Open Mode)	None	1
66.249.65.168	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
157.55.39.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in aka.idf.il/ishurim/cityofficers/	None	1
64.62.219.71	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
105.203.254.4	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
79.176.88.206	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
109.65.147.109	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.6.161	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
89.138.190.55	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.49	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
77.138.243.23	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
66.249.69.116	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/01022011tutim.aspx	Block	1
176.13.17.176	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
64.62.219.76	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
105.203.254.6	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.176.88.206	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
66.249.64.142	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
46.19.85.110	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
89.237.68.93	France	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
79.176.32.168	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.76.47	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/templates/www.behazdaa.org	Block	1
64.62.219.98	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.246.133.148	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.76.98	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
66.249.65.163	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
46.116.198.123	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
105.203.254.1	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.176.88.206	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 79.176.88.206	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
199.30.24.208	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
105.203.254.11	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
64.62.219.165	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
74.6.53.161	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1

08-21-2016-20:04:08 to 08-21-2016-21:04:08