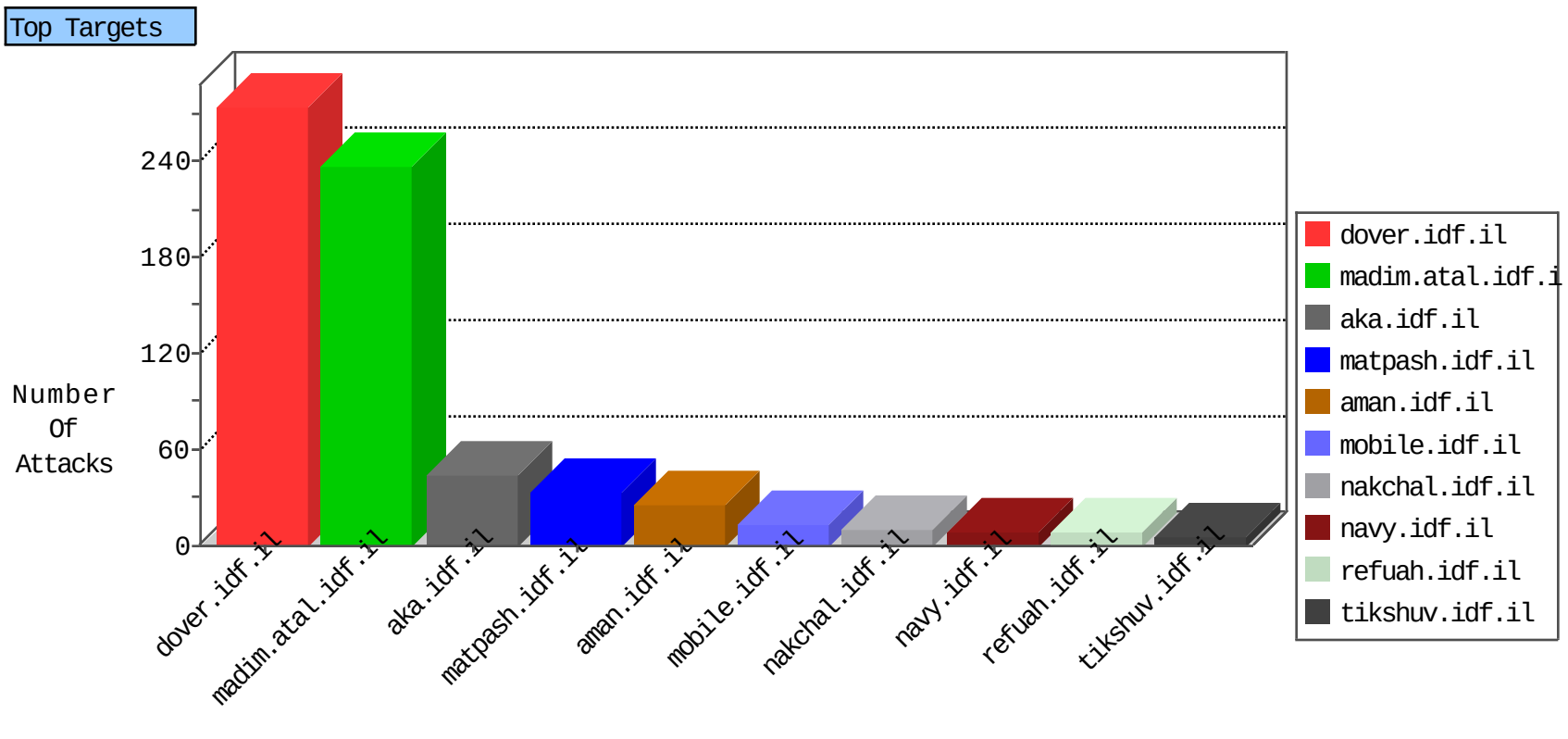
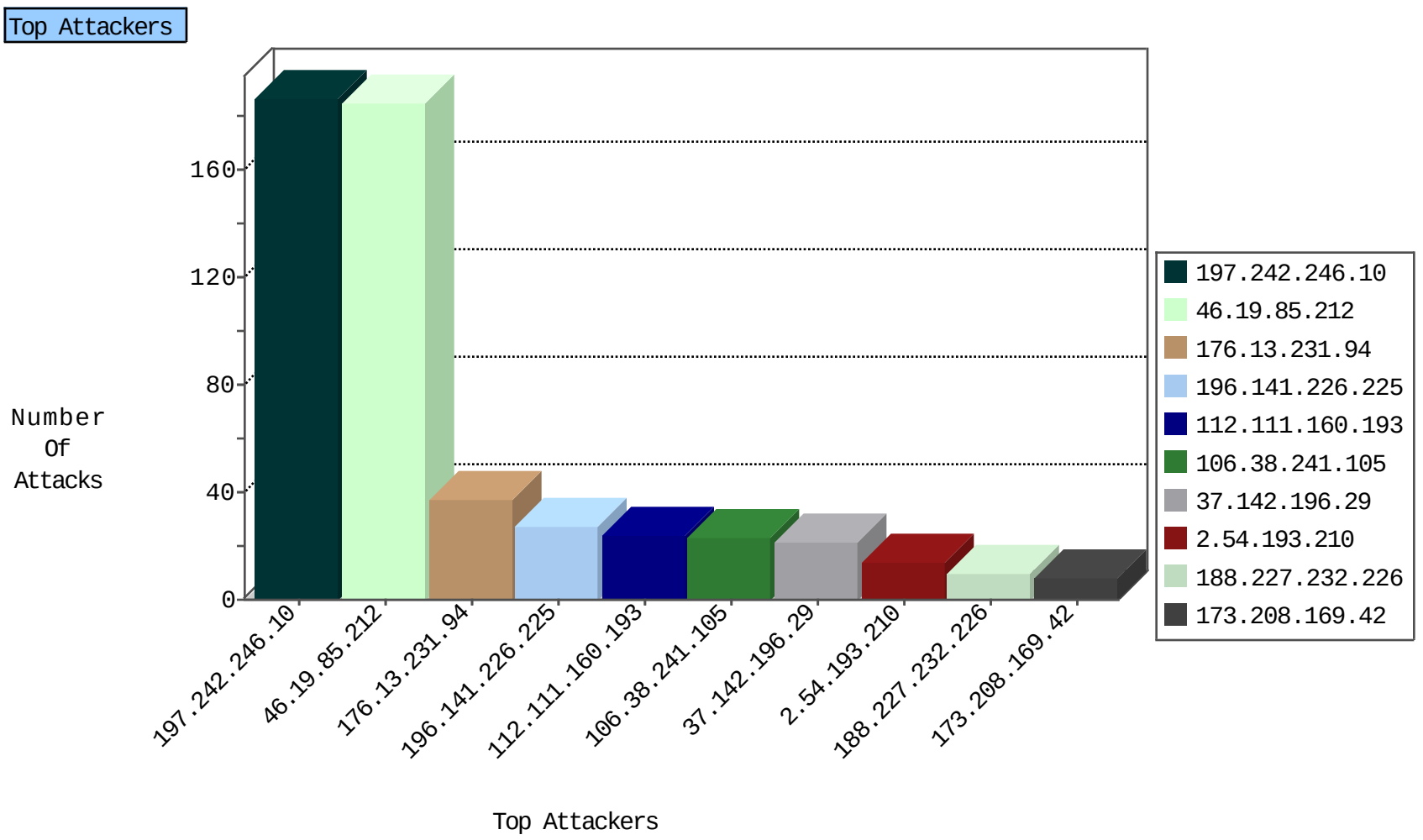
08-30-2016-20:04:03 to 08-30-2016-21:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-30-2016-20:04:03 to 08-30-2016-21:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.242.246.10	Nigeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	47
80.74.123.50	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15
79.179.63.219	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
109.253.246.78	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
79.180.51.68	Israel	147.237.72.166	aka.idf.il	Black List	drop	2

08-30-2016-20:04:03 to 08-30-2016-21:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	21
173.208.169.42	United States	147.237.76.86	navy.idf.il	C1000125: HTTP: Block admin login to gov.il sites ?q=user	Permit	8

08-30-2016-20:04:03 to 08-30-2016-21:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
111.198.181.2	147.237.77.178	China	e.matpash.idf.il	GPL SCAN nmap TCP	2
36.110.67.130	147.237.77.178	China	e.matpash.idf.il	GPL SCAN nmap TCP	2
46.227.67.172	147.237.72.217	Sweden	e.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.188.150	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.129.160.229	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
106.38.241.105	147.237.72.156	China	aman.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.227.67.172	147.237.77.234	Sweden	halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
191.32.230.77	147.237.72.166	Brazil	aka.idf.il	portscan: TCP Distributed Portscan	1
139.162.13.205	147.237.77.235	Singapore	sviva.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
109.253.138.188	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1

08-30-2016-20:04:03 to 08-30-2016-21:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.242.246.10	Nigeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	184
196.141.226.225	Egypt	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	27
2.54.193.210	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	10
46.19.86.141	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
188.227.232.226	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
212.179.219.26	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
188.227.232.226	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	4
2.54.193.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
194.90.66.9	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
37.46.41.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.8.117	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
109.253.146.253	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.133.41	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	2
109.253.212.218	Israel	147.237.72.167	ishurim.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
176.13.241.108	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.145.227	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.35	akaws.idf.il	drop		drop	1
176.13.15.165	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.192.0	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.233.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
89.139.172.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.195.185	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.234.60	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

08-30-2016-20:04:03 to 08-30-2016-21:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.212	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	185
176.13.231.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
37.142.196.29	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	21
112.111.160.193	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 112.111.160.193	Block	17
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.183.235	Block	6
2.55.25.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
112.111.160.193	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
192.187.101.170	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.187.101.170	Block	4
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.19.86.1	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.202.113	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.53.182.212	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.177.132.218	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 79.177.132.218	Block	2
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
79.177.132.218	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/8/	Block	2
109.67.181.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.199	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
139.162.13.205	Singapore	147.237.77.235	sviva.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	2
2.53.166.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
66.249.64.22	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
176.13.229.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
192.169.7.223	United States	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/	Block	1
74.125.76.32	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/login/	Block	1
109.64.83.223	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.19.85.92	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
82.81.106.129	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
74.125.76.33	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/giyus/login/	Block	1
112.111.160.193	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
46.116.21.201	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
85.65.183.235	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
176.193.59.246	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/kiosk/printablekiosk.aspx	Block	1
82.81.106.129	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 82.81.106.129	Block	1
192.187.101.170	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/assets/elfinder/elfinder.html	Block	1
77.138.115.17	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
46.117.24.178	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
128.177.161.159	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
5.28.167.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.75.140.166	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
79.181.227.8	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.23.164.156	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
2.53.130.147	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
82.81.160.227	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
194.219.99.138	Greece	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
77.139.6.178	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	1
66.102.9.2	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
31.173.80.158	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
95.135.149.243	Ukraine	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
80.179.225.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

08-30-2016-20:04:03 to 08-30-2016-21:04:03