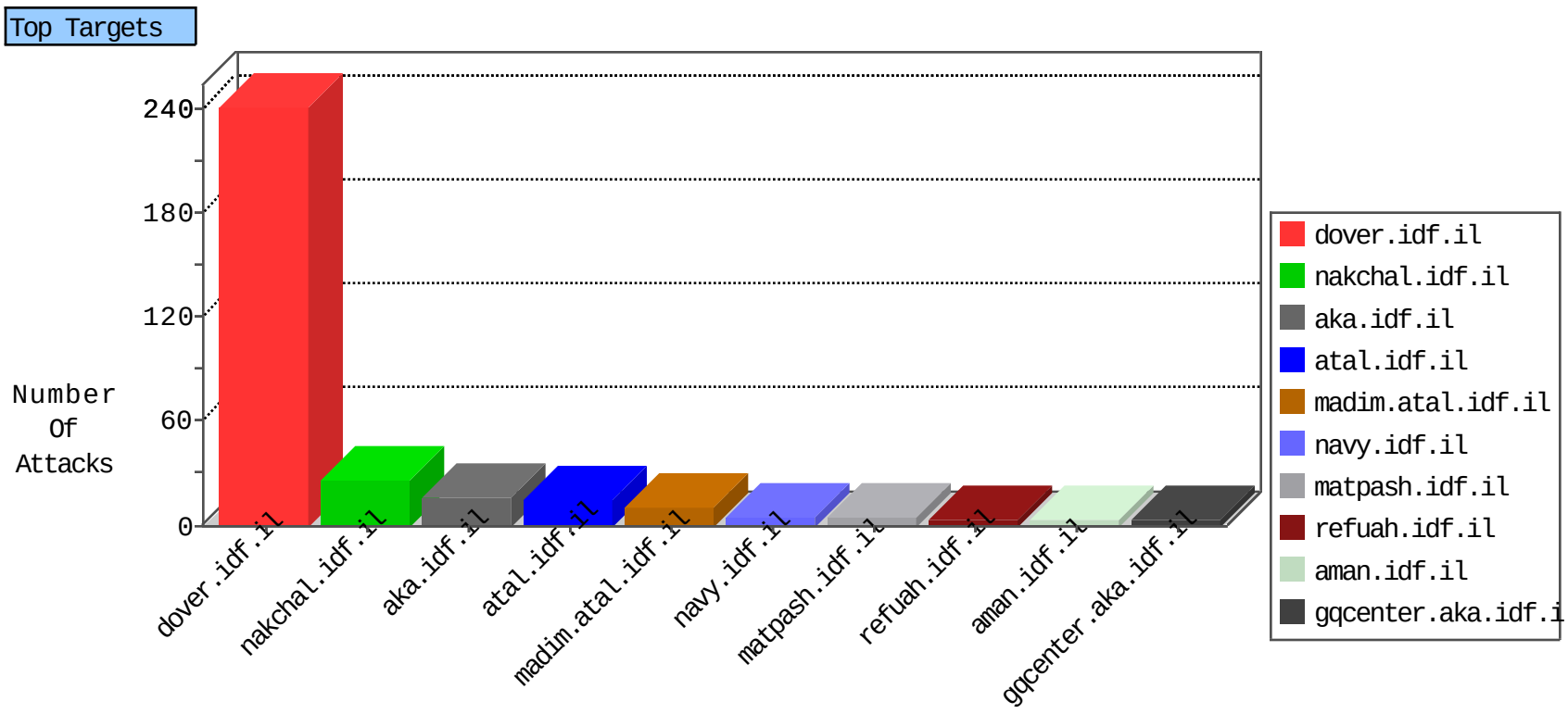
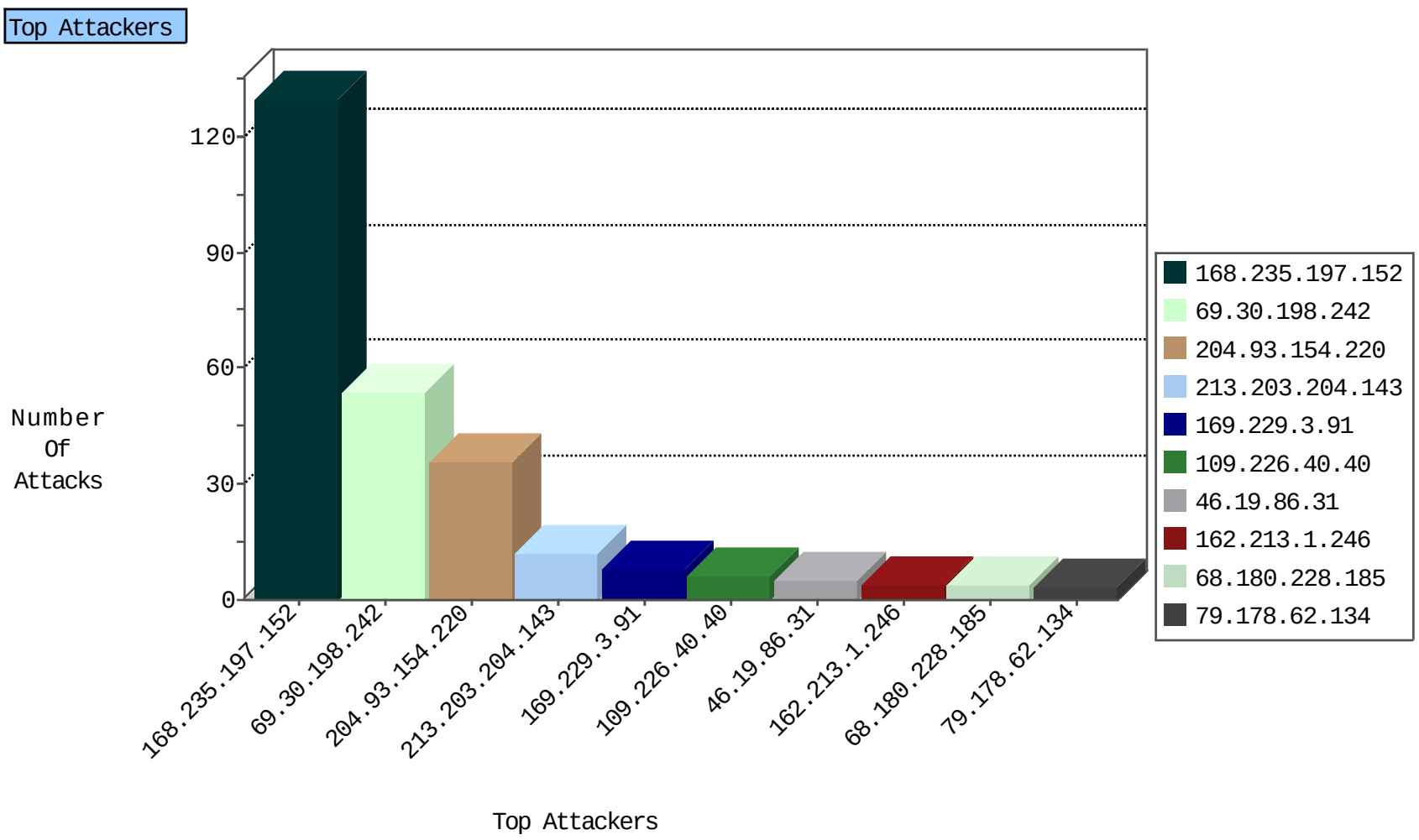
08-21-2016-22:04:04 to 08-21-2016-23:04:04

IDF Under Attack Daily Report





08-21-2016-22:04:04 to 08-21-2016-23:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.220	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	157
109.226.40.40	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
2.53.28.11	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
68.180.228.185	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
168.235.197.152	United States	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	3
79.178.62.134	Israel	147.237.77.216	dover.idf.il	Black List	drop	3
58.218.204.245	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
31.154.81.12	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
84.109.8.231	Israel	147.237.77.216	dover.idf.il	Black List	drop	1

08-21-2016-22:04:04 to 08-21-2016-23:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.198.242	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	28
69.30.198.242	United States	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	21
213.203.204.143	Germany	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
69.30.198.242	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	5
123.126.68.130	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
51.255.65.56	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
164.132.161.69	Italy	147.237.77.234	halag.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
195.228.45.176	Hungary	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1
198.20.69.74	United States	147.237.0.16	my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

08-21-2016-22:04:04 to 08-21-2016-23:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.203.204.143	147.237.77.233	Germany	atal.idf.il	SQL Injection - Select From	6
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	4
151.80.40.87	147.237.77.176	France	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2

08-21-2016-22:04:04 to 08-21-2016-23:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.197.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	127
46.19.86.31	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
67.140.235.121	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
81.218.66.211	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
2.55.133.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.135.222	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
5.29.146.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.102.242.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.178.235.99	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.216.149	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.242.142	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.8.27	e.madim.atal.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.201	e.atal.idf.il	drop	SAM rule	drop	1
141.212.122.18	United States	147.237.0.200	m4u.idf.il	drop		drop	1
61.240.144.65	China	147.237.8.50	e.tikshuv.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
109.253.128.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	1
141.212.122.19	United States	147.237.0.200	m4u.idf.il	drop		drop	1
61.240.144.65	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
213.8.204.32	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
173.255.244.48	United States	147.237.0.35	akaws.idf.il	drop		drop	1
216.243.31.2	United States	147.237.0.35	akaws.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
109.253.213.87	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.6.148	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1

08-21-2016-22:04:04 to 08-21-2016-23:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.29.39	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
2.53.49.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.149.224	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.106	Block	2
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.112	Block	2
84.94.76.76	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/mail/sachar	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
109.64.114.45	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
77.138.209.150	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
46.117.6.17	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
185.120.124.34	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
84.94.49.131	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
109.67.191.114	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/haredim/general.aspx	Block	1
79.179.201.50	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/imagevideogallerylobby/imagevideogallerylobby.js	Block	1
207.46.13.20	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
131.253.26.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.180.163.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/scroller/jquery.jcarousel.js	Block	1
212.59.115.6	Russian Federation	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
87.71.39.90	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	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
149.56.223.98	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/blog/	Block	1
81.218.204.190	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	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
213.57.204.33	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
89.138.149.242	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
37.26.149.229	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
157.55.39.12	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/recruitinformation	Block	1
81.255.154.161	France	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1

08-21-2016-22:04:04 to 08-21-2016-23:04:04