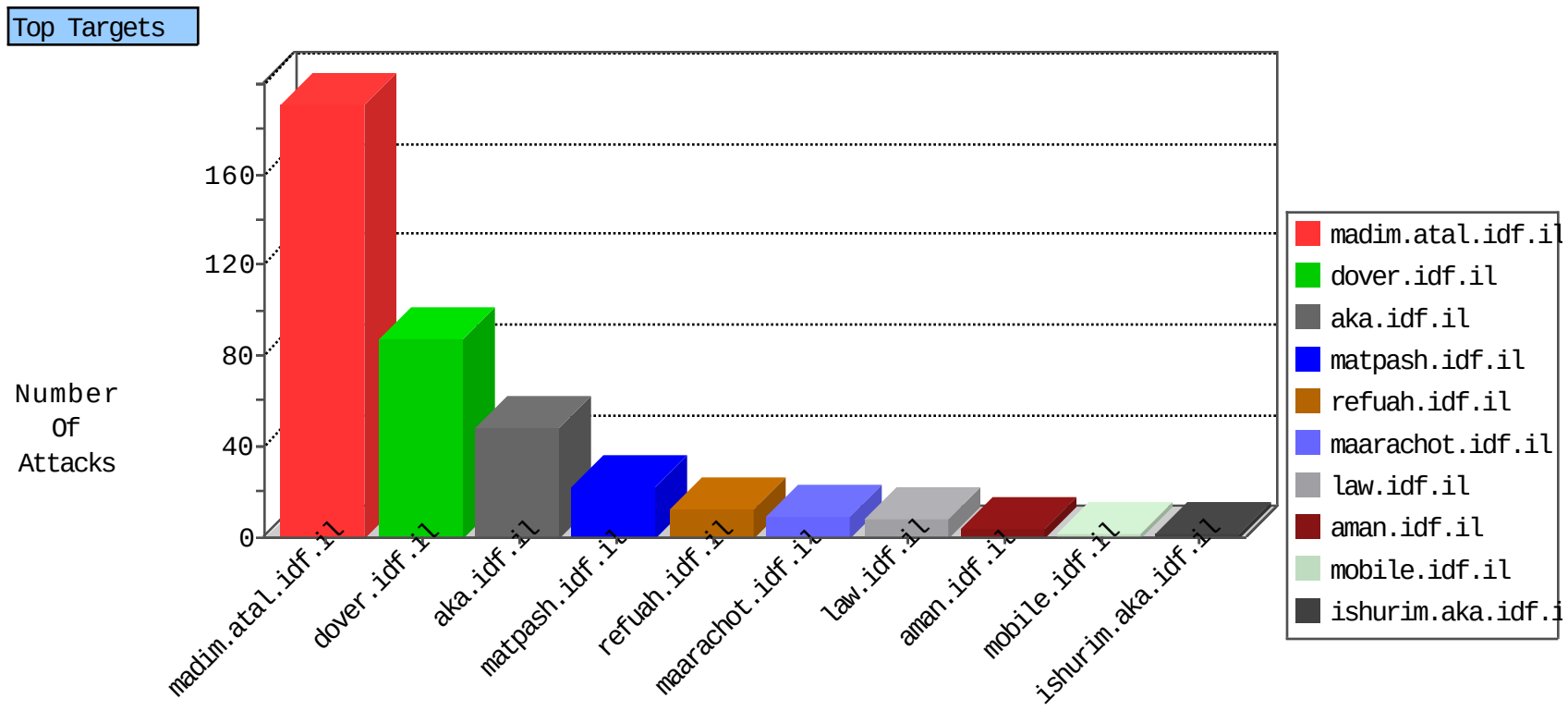
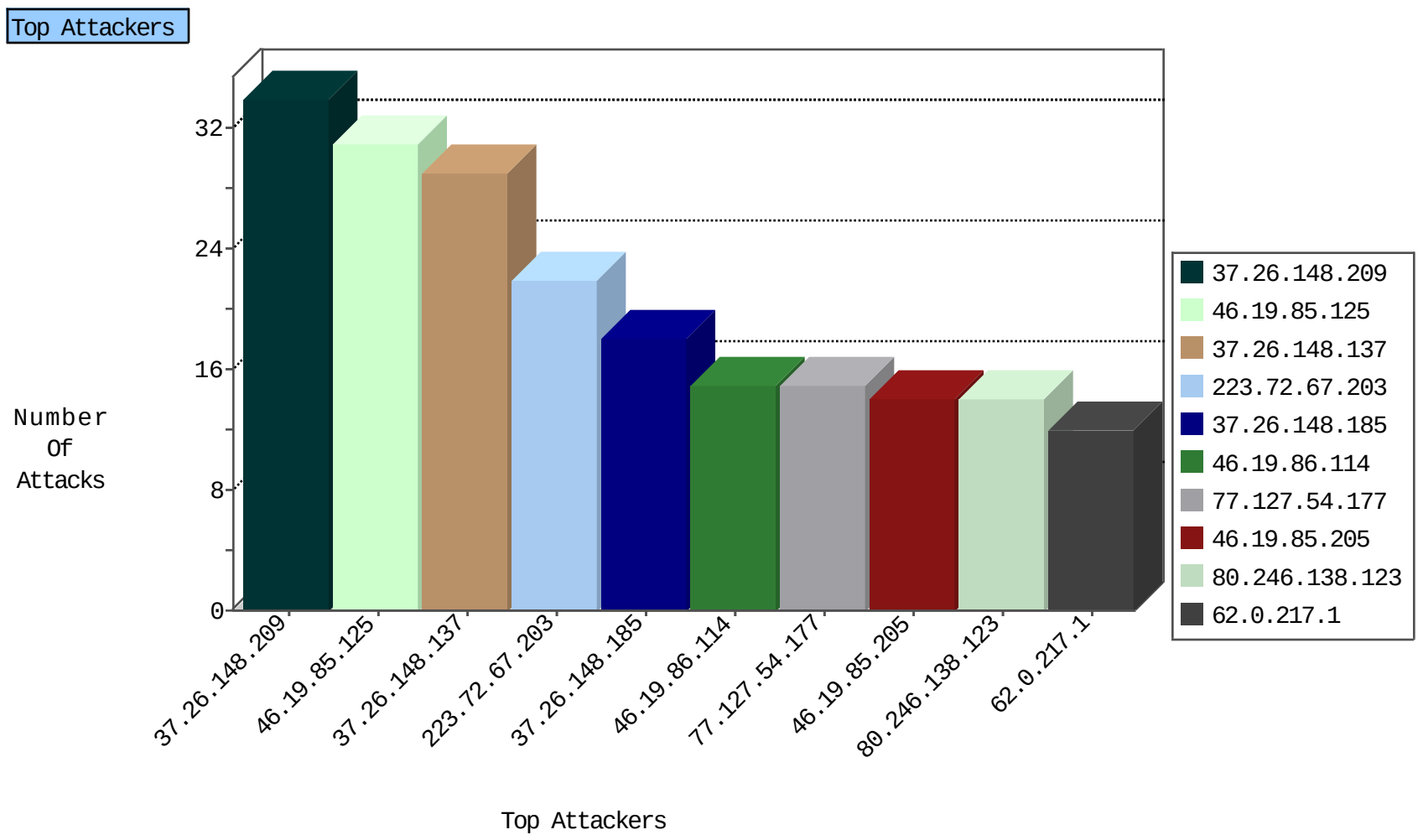
08-22-2016-10:04:09 to 08-22-2016-11:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-22-2016-10:04:09 to 08-22-2016-11:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.253.91.179	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	2
93.174.95.106	Netherlands	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
94.102.49.190	Netherlands	147.237.76.30	himush.idf.il	Black List	drop	1

08-22-2016-10:04:09 to 08-22-2016-11:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.129	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

08-22-2016-10:04:09 to 08-22-2016-11:04:09

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	3
82.81.76.144	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	1

08-22-2016-10:04:09 to 08-22-2016-11:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
62.0.217.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
62.0.211.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.179.177.8	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
193.43.246.250	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
62.219.154.218	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	5
109.253.134.84	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
93.72.88.11	Ukraine	147.237.77.216	dover.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	4
213.6.42.6	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.76	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.232.132.51	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
178.233.88.108	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.11.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.200	m4u.idf.il	drop	SAM rule	drop	1
176.13.233.61	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
207.232.27.5	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
176.13.243.225	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
109.253.215.31	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	1
120.132.67.190	China	147.237.0.33	idf.il	drop		drop	1
45.79.156.96	United States	147.237.0.35	akaws.idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	34
46.19.85.125	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
37.26.148.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
37.26.148.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
46.19.86.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
77.127.54.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
223.72.67.203	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 223.72.67.203	Block	15
46.19.85.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
80.246.138.123	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
223.72.67.203	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	6
2.55.174.150	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.253.91.179	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	4
37.26.148.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
2.55.163.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.146.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.130.68	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.55.180.3	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.55.150.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.202.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
185.120.125.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.112	Block	2
82.81.161.50	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.55.149.225	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
212.25.102.63	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/images/1.he/infocenteritem/	Block	2
79.178.0.251	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.178.0.251	Block	2
145.130.25.230	Netherlands	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
212.25.102.63	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/205-he/patzar.aspx	Block	2
185.120.125.119	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 185.120.125.119	Block	2
46.121.65.118	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	2
77.138.25.117	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	2
145.130.25.230	Netherlands	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
46.19.85.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.25.102.63	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/657-he/patzar.aspx	Block	2
2.55.133.127	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
77.138.46.180	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
2.53.141.51	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
173.186.135.99	United States	147.237.72.166	aka.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/sip_storage/files/6/3416.jpg	Block	1
46.19.86.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.81.76.144	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/smalim/	Block	1
79.177.37.157	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
213.91.213.66	Bulgaria	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.55.136.41	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.198.151.45	Europe	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
109.253.221.7	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
46.135.229.10	Czech Republic	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.135.229.10	Block	1
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl17 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
77.138.140.81	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/3295.jpg	Block	1