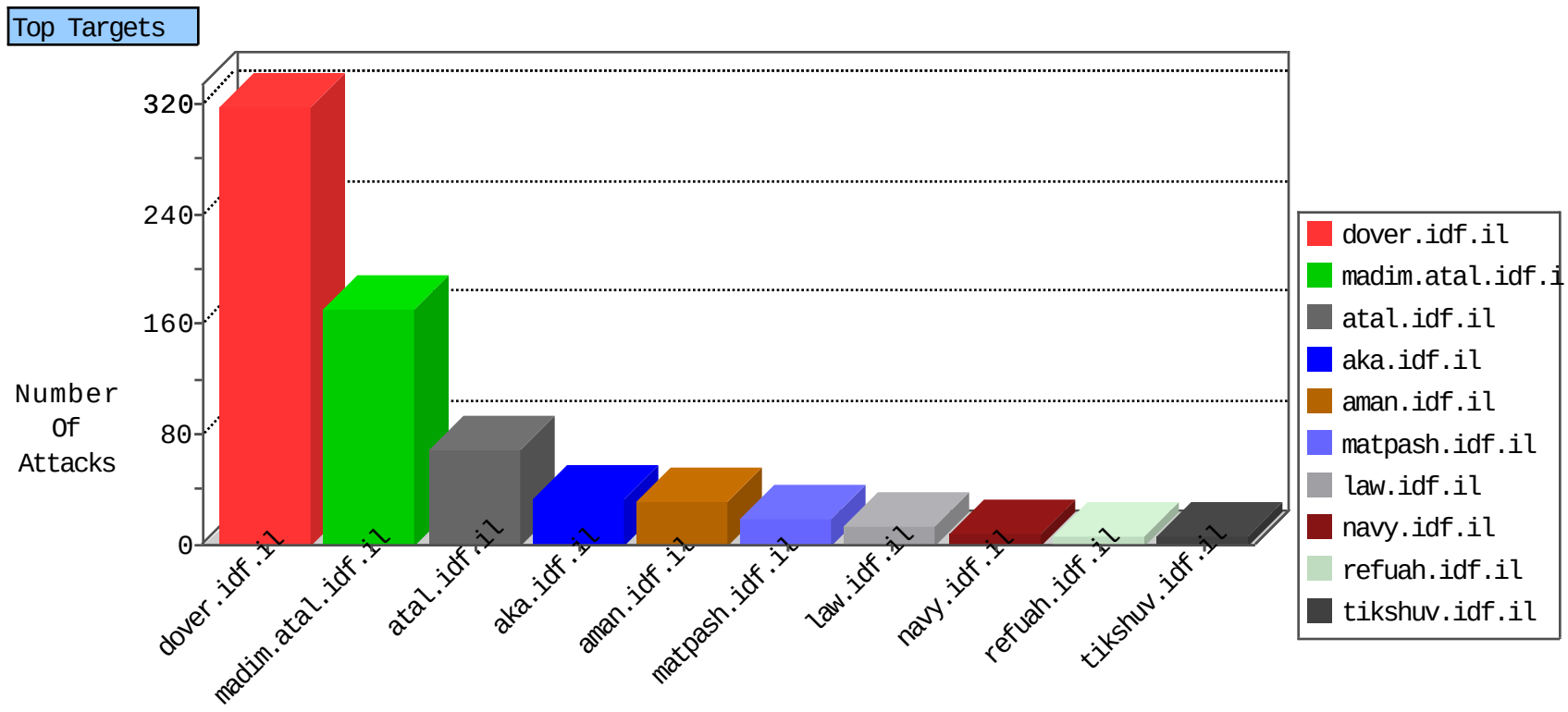
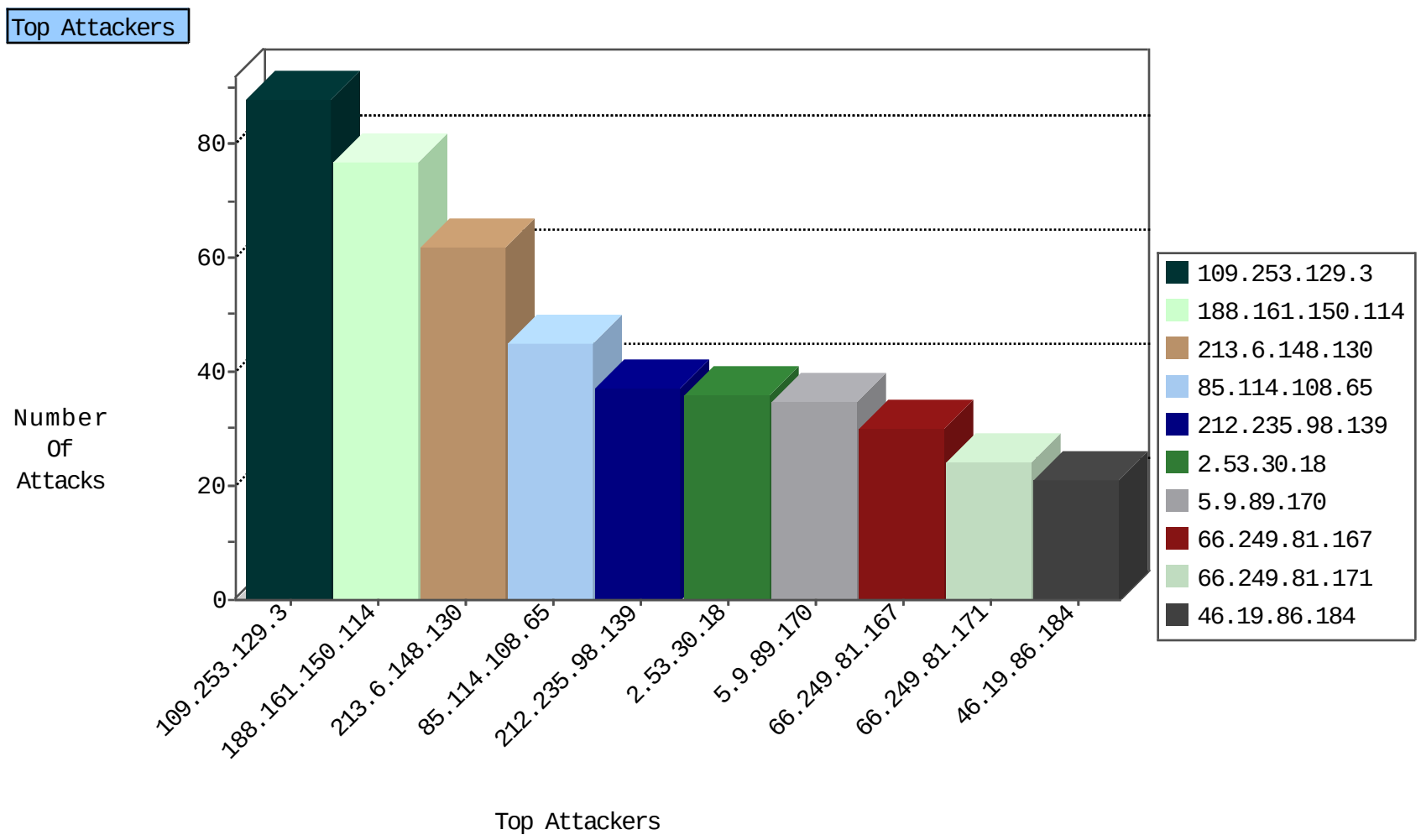
08-22-2016-14:04:10 to 08-22-2016-15:04:10

IDF Under Attack
Daily Report

Top Targets



Top Attackers



08-22-2016-14:04:10 to 08-22-2016-15:04:10

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.161.150.114	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	4035
213.6.148.130	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	2034
85.114.108.65	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	2014
2.55.154.62	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
2.55.174.239	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
2.55.138.186	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
2.55.188.12	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
134.191.232.70	Israel	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	4
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
77.138.229.183	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
71.6.165.200	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
89.139.232.81	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
188.161.150.114	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
93.174.93.156	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1
192.81.135.222	United States	147.237.8.28	e.mobile-ks.idf.il	JLM_Purple_Con_Limit_Https	drop	1

08-22-2016-14:04:10 to 08-22-2016-15:04:10

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.89.170	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	14
5.9.89.170	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	10
5.9.89.170	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	7
5.9.89.170	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
46.119.117.90	Ukraine	147.237.77.216	dover.idf.il	15323: HTTP: User-Agent (MRSPUTNIK)	Block	3

08-22-2016-14:04:10 to 08-22-2016-15:04:10

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.6.148.130	147.237.77.216	Palestinian Territory, Occupied	dover.idf.i	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

08-22-2016-14:04:10 to 08-22-2016-15:04:10

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.81.167	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	30
66.249.81.171	Poland	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	24
66.249.81.163	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	12
85.64.170.165	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
46.32.121.5	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
62.219.52.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.64.54.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.213.5	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
87.68.26.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.91	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
207.232.1.104	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
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.0.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.100.230.90	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
169.229.3.91	United States	147.237.0.35	akaws.idf.il	drop	SAM rule	drop	1
188.161.150.114	Palestinian Territory, Occupied	147.237.76.34	yohalan.idf.il	drop		drop	1
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
192.116.4.99	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.76.201	e.atal.idf.il	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
193.169.70.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.226.162.61	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
184.105.247.247	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1

08-22-2016-14:04:10 to 08-22-2016-15:04:10

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.129.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	88
2.53.30.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
46.19.86.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
77.139.102.77	France	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	10
109.253.209.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
212.199.240.148	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 212.199.240.148	Block	5
109.253.216.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.11.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.102.77	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	3
87.71.32.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.165.116	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
217.132.14.77	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
80.246.130.164	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.139.102.77	France	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
217.132.147.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.68.35.54	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	2
80.246.133.12	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	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
176.13.15.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.130.57	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.184.112	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
80.246.133.197	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
77.139.119.110	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in Header Name	Block	1
109.67.202.188	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
89.139.230.6	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
5.29.247.206	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
176.13.236.185	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.53.134.21	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	NULL Character in Method	Block	1
80.246.130.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
213.57.7.4	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	1
109.65.41.13	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.65.41.13	Block	1
2.53.184.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Malformed URL	Block	1
80.246.138.183	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/registrationwizard/register.aspx parameter	None	1
77.139.180.13	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in Method ý4àc[[#2]]Ë[[#31]]œiÀÇú[[#20]]jþ]Œã¢oî3wÂí…Åz[âãâHG[[#11]]â†«áQ{«X‡Ä	Block	1
109.67.202.188	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
91.231.192.149	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
188.161.150.114	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	Block	1
2.53.138.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.76.147	chinuch.aka.idf.il	Illegal Byte Code Character in Method	Block	1
80.246.130.140	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
117.216.140.129	India	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1

08-22-2016-14:04:10 to 08-22-2016-15:04:10