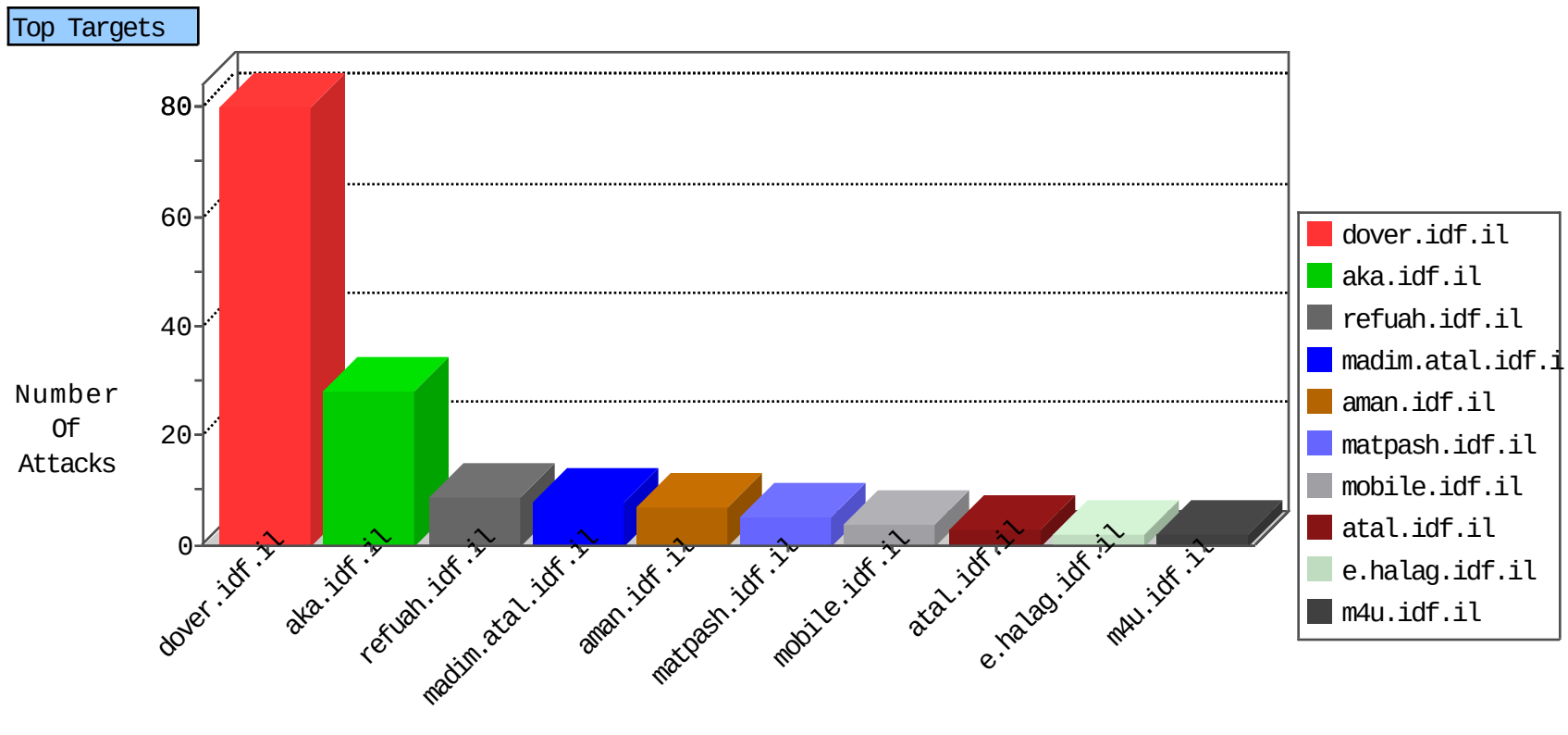
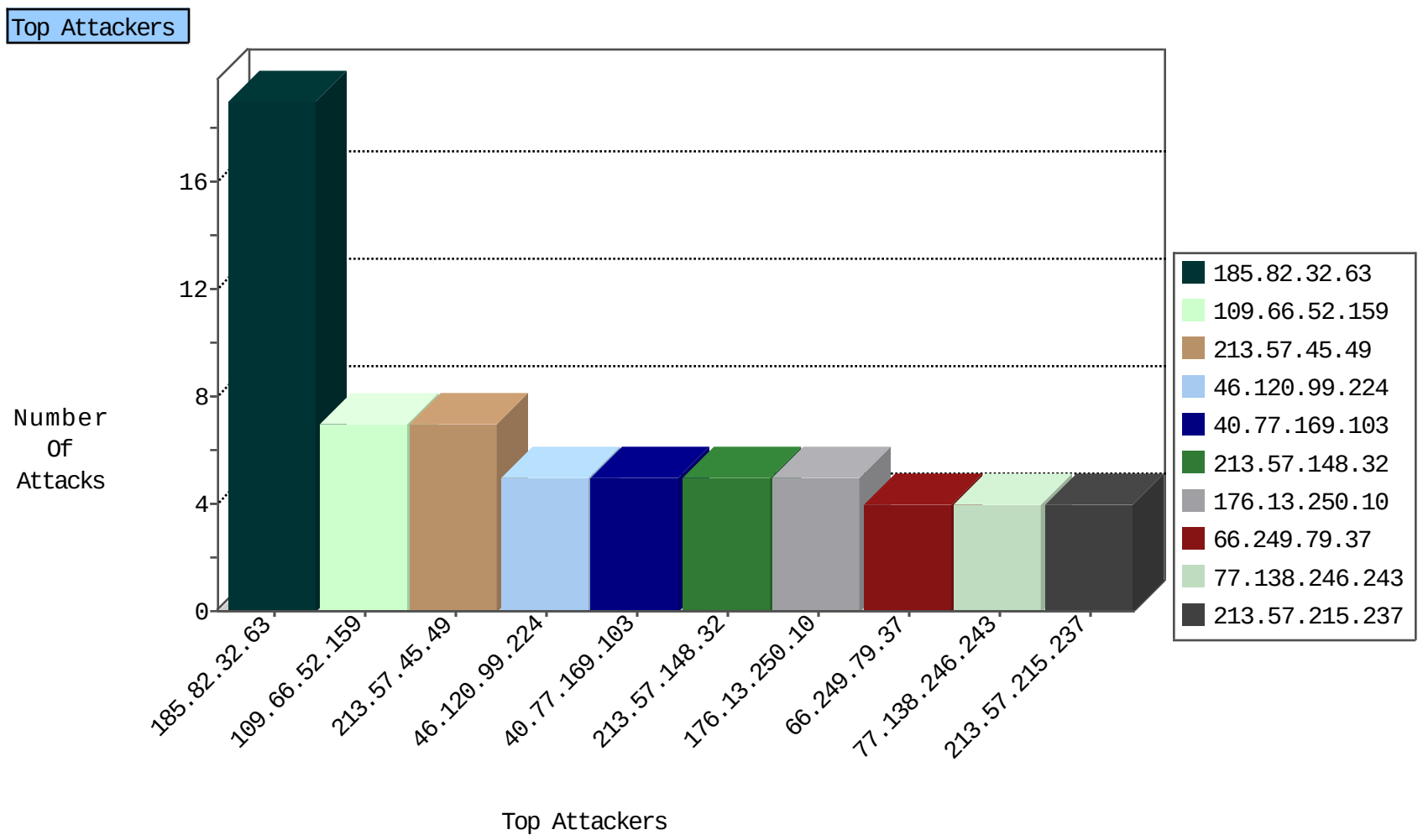
08-23-2016-21:04:03 to 08-23-2016-22:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-23-2016-21:04:03 to 08-23-2016-22:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
213.57.45.49	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
213.57.148.32	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
46.120.99.224	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
84.109.32.240	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
205.203.135.1	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
89.248.168.21	Netherlands	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.86	navy.idf.il	Black List	drop	1
89.248.168.21	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	1
89.248.168.21	Netherlands	147.237.76.198	e.yohalan.idf.il	Black List	drop	1

08-23-2016-21:04:03 to 08-23-2016-22:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.130	United States	147.237.72.166	aka.idf.i	C1000074: HTTP: majestic bot	Permit	2
81.213.227.27	Turkey	147.237.72.166	aka.idf.i	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1
81.213.227.27	Turkey	147.237.72.166	aka.idf.i	C1000016: HTTP: administrator in URI	Permit	1

08-23-2016-21:04:03 to 08-23-2016-22:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.66.52.159	147.237.76.42	Israel	refuah.idf.il	ET SCAN NMAP -sA (2)	7
81.213.227.27	147.237.72.166	Turkey	aka.idf.il	SERVER-WEBAPP admin.php access	1
212.76.112.216	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
211.23.156.152	147.237.76.202	Taiwan	e.halag.idf.il	ET SCAN Potential SSH Scan	1
195.88.208.193	147.237.77.179	Russian Federation	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
133.242.4.52	147.237.76.42	Japan	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.76.202	Japan	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
95.211.217.224	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
85.250.173.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.224.109.175	147.237.0.16	Germany	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
211.23.156.152	147.237.77.233	Taiwan	atal.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.98	147.237.76.39	United States	mobile.meitav.idf.il	ET DROP Dshield Block Listed Source	1
176.47.22.181	147.237.77.216	Saudi Arabia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
133.242.3.168	147.237.8.45	Japan	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
95.211.217.224	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1

08-23-2016-21:04:03 to 08-23-2016-22:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
185.82.32.63	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
157.55.39.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
87.69.94.255	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.230.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.199.93.122	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
77.139.190.82	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.22.130.86	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.129	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
81.64.3.151	France	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
194.181.182.195	Poland	147.237.76.34	yohalan.idf.il	drop		drop	1
176.13.249.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.146.92	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.69	United States	147.237.0.200	m4u.idf.il	drop		drop	1
185.125.4.222	Poland	147.237.0.15	kosher-kravi.idf.il	drop	SAM rule	drop	1
141.212.122.70	United States	147.237.0.200	m4u.idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.250.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
213.57.215.237	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	4
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.37	Block	4
109.253.142.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
190.80.123.191	Guyana	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/cityofficers/	Block	2
77.138.3.6	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/exampcert/	Block	2
77.138.246.243	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.246.243	Block	2
77.138.246.243	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	2
212.34.20.89	Jordan	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
66.249.66.146	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/apple-app-site-association	Block	1
85.219.143.195	Poland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
46.19.86.103	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
197.49.168.86	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.139.202.210	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
212.34.20.89	Jordan	147.237.77.216	dover.idf.il	Malformed URL http/1.1	Block	1
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/7/שקופית 10	Block	1
93.94.88.30	Italy	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.117.212.104	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
207.46.13.39	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
157.55.39.110	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.177.17.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
212.34.20.89	Jordan	147.237.77.216	dover.idf.il	Unknown HTTP Request Method /6/9466.jpg in URL www.idf.ilhttp/1.1	Block	1
66.249.76.46	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.46	Block	1
192.198.151.43	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
95.86.86.3	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
77.138.243.23	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
46.120.178.60	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl09 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
207.46.13.41	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/112435.pdf).	Block	1
157.55.39.194	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20705-he/dover	Block	1
80.178.83.12	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
212.76.112.216	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.76.111	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
5.22.135.105	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
192.243.55.136	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	1
109.65.7.102	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.147.244.101	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
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
176.13.1.229	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.108.88.5	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.85.71	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
197.48.45.179	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.252.29.59	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

08-23-2016-21:04:03 to 08-23-2016-22:04:03