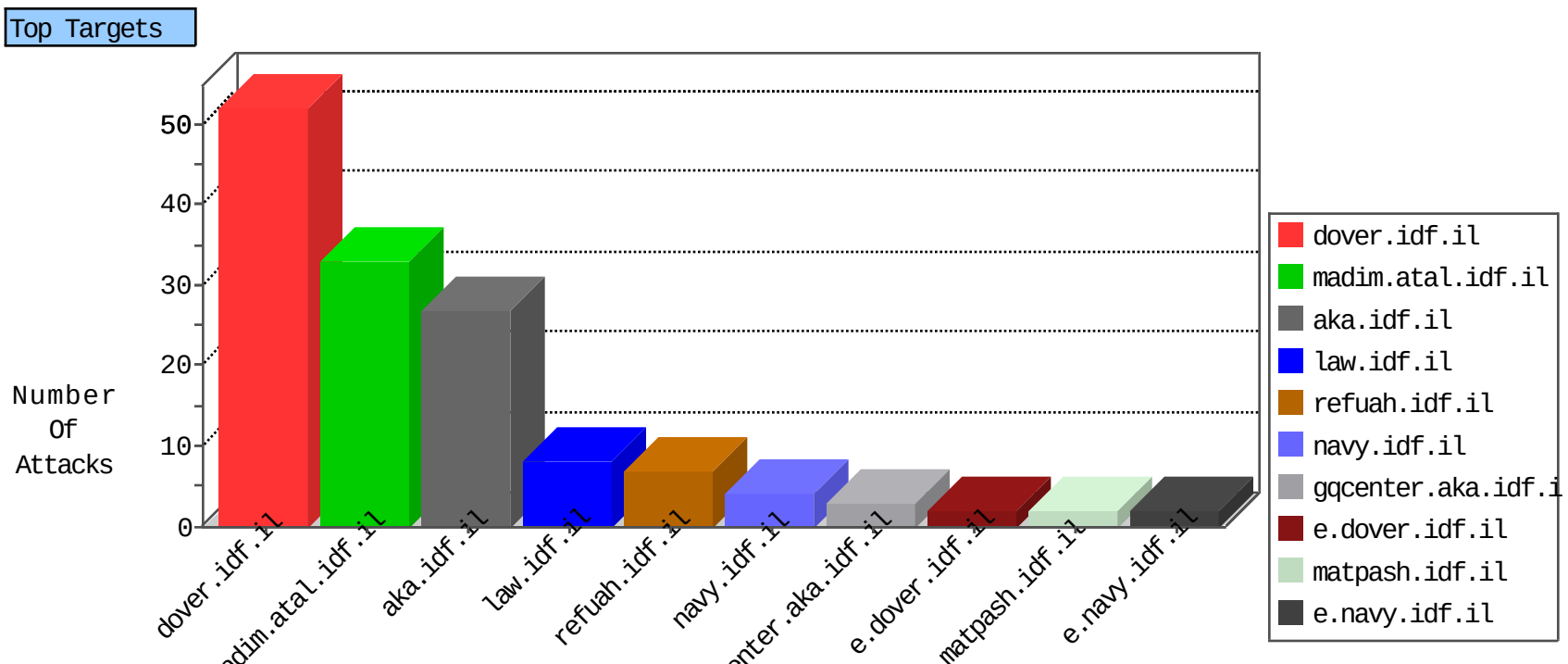
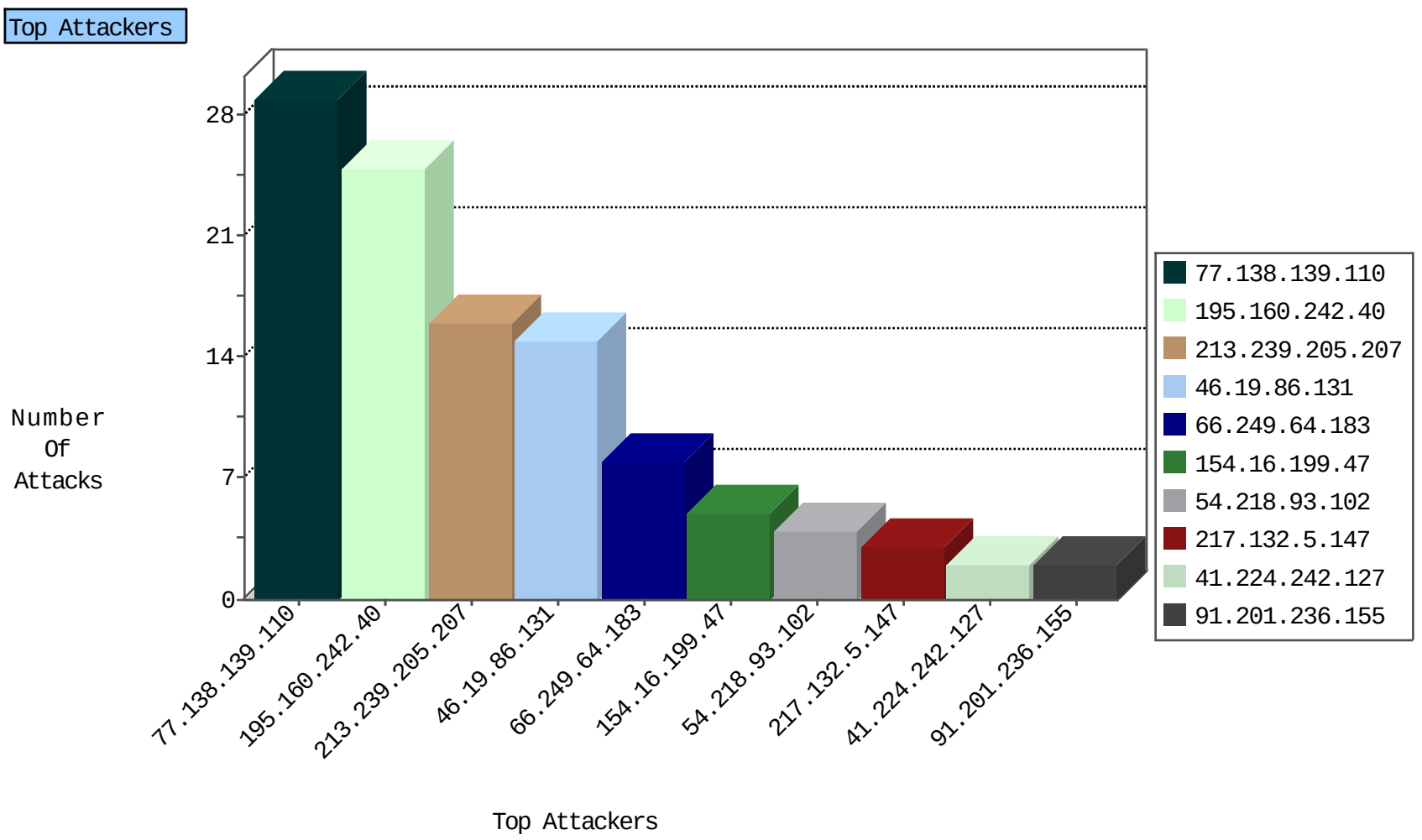
08-19-2016-21:04:06 to 08-19-2016-22:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-19-2016-21:04:06 to 08-19-2016-22:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
179.32.74.126	Colombia	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
61.178.42.242	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
175.181.34.65	Taiwan	147.237.77.243	mobile.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1

08-19-2016-21:04:06 to 08-19-2016-22:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
164.132.161.29	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-19-2016-21:04:06 to 08-19-2016-22:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
54.218.93.102	147.237.77.216	United States	dover.idf.il	Xenu Link Sleuth User Agent	4
186.240.158.133	147.237.77.216	Brazil	dover.idf.il	Xenu Link Sleuth User Agent	2
94.102.48.195	147.237.76.86	Netherlands	navy.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.76.176	Ukraine	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.149	147.237.8.27	Ukraine	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
41.224.242.127	147.237.76.148	Tunisia	gqcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
173.208.249.37	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
154.16.199.47	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
154.16.199.47	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1
154.16.199.47	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
66.249.93.71	147.237.76.42	Europe	refuah.idf.il	ET SCAN NMAP -sA (2)	1
46.172.71.251	147.237.76.201	Ukraine	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
209.95.143.10	147.237.76.31	United States	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
41.224.242.127	147.237.76.148	Tunisia	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
5.255.90.133	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 1024	1
173.208.249.37	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
154.16.199.47	147.237.77.61	United States	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
154.16.199.47	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1

08-19-2016-21:04:06 to 08-19-2016-22:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.19.86.131	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
213.239.205.207	Germany	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
213.239.205.207	Germany	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	2
37.232.29.66	Georgia	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
213.239.205.207	Germany	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
213.239.205.207	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
213.239.205.207	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
213.239.205.207	Germany	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	2
213.239.205.207	Germany	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.233.78	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.0.200	m4u.idf.il	drop	SAM rule	drop	1
77.127.79.208	Israel	147.237.72.156	aman.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
109.253.136.87	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

08-19-2016-21:04:06 to 08-19-2016-22:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.138.139.110	France	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	7
217.132.5.147	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/580-he/patzar.aspx	Block	2
89.138.35.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.27.105.64	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
68.180.228.185	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
66.249.64.171	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
207.46.13.25	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/smalim/showbig.aspx	None	1
84.111.2.11	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.111.2.11	Block	1
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.183	Block	1
5.22.135.174	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
131.253.27.159	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.229.39	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
66.249.64.174	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/templates/news/news.aspx	Block	1
217.132.5.147	Israel	147.237.77.74	law.idf.il	Parameter Type Violation FreeText in www.law.idf.il/421-he/patzar.aspx	Block	1
84.111.2.11	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	1
66.249.76.51	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
66.69.107.199	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
157.55.39.110	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
66.249.64.180	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-9067-he/atal.aspx	Block	1
85.64.170.207	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
66.249.76.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.102.9.76	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
157.55.39.176	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.181.70.248	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.64.182	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.79.141	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
66.102.9.95	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
79.181.70.248	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
2.53.180.107	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1
109.64.10.225	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1

08-19-2016-21:04:06 to 08-19-2016-22:04:06