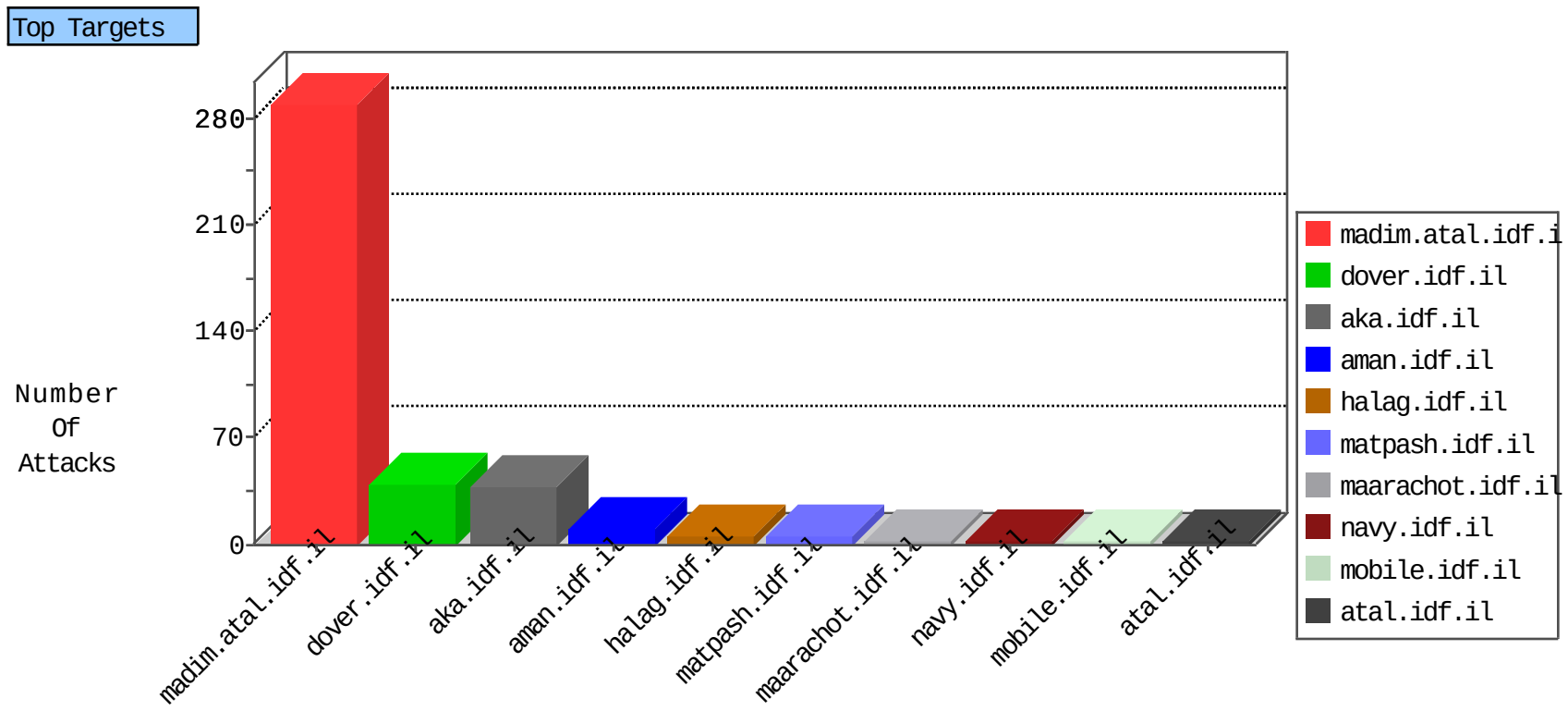
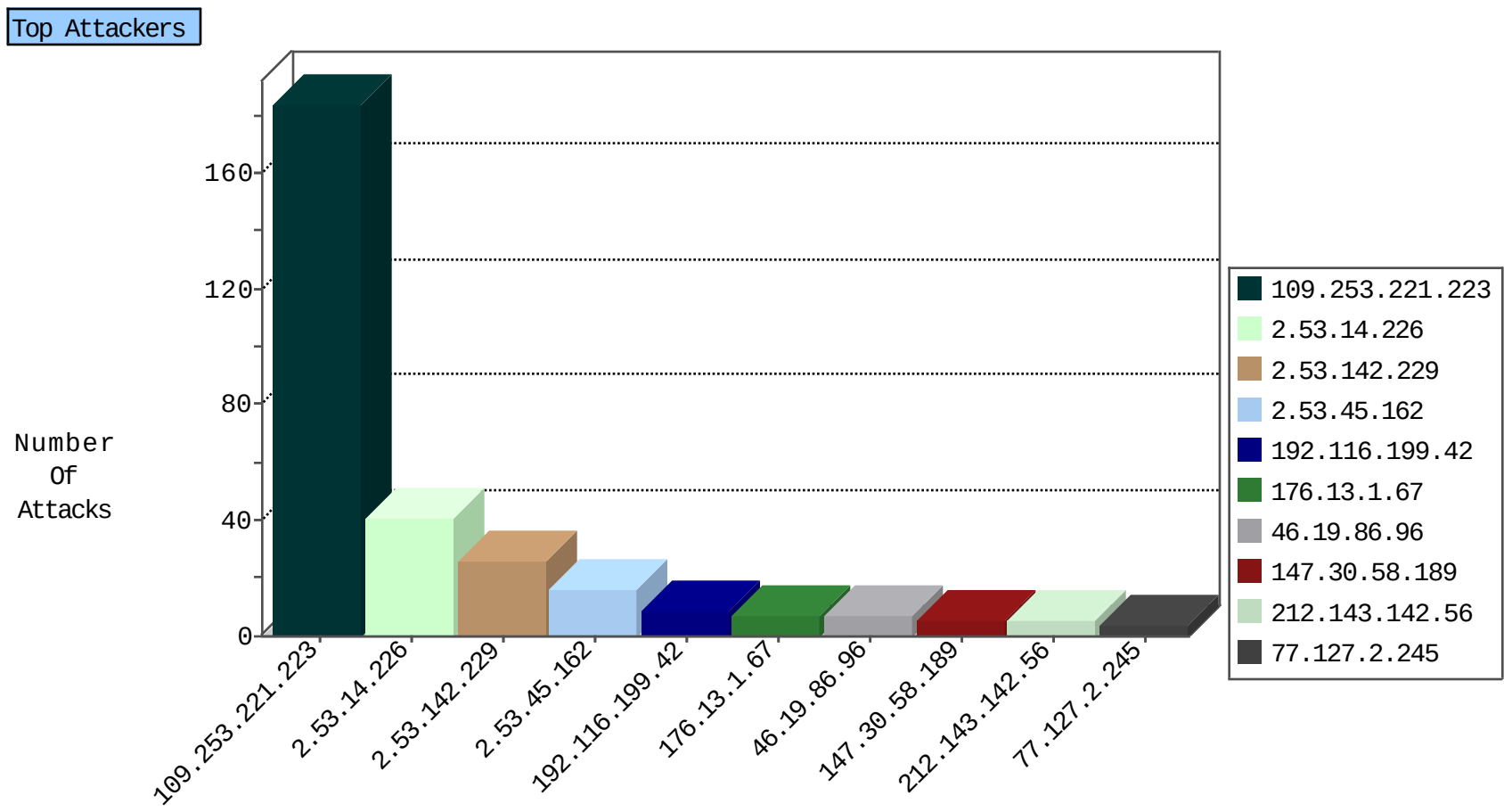
08-17-2016-18:04:05 to 08-17-2016-19:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-17-2016-18:04:05 to 08-17-2016-19:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.177.205	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
2.53.184.135	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	1
154.16.199.47	United States	147.237.76.86	navy.idf.il	Black List	drop	1

08-17-2016-18:04:05 to 08-17-2016-19:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
164.132.161.75	Italy	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-17-2016-18:04:05 to 08-17-2016-19:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
176.228.94.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.108.10.31	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
66.249.76.52	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
31.154.42.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
206.47.151.114	147.237.76.177	Canada	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
116.108.2.218	147.237.76.30	Vietnam	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
87.236.194.161	147.237.77.233	Czech Republic	atal.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.78.31	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	1
32.210.150.71	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
1.164.24.97	147.237.8.46	Taiwan	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
213.14.143.15	147.237.76.31	Turkey	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

08-17-2016-18:04:05 to 08-17-2016-19:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.116.199.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
176.13.1.67	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
147.30.58.189	Kazakstan	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
185.120.126.14	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
147.30.58.189	Kazakstan	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
109.253.201.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.5.9	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
5.22.130.97	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.21.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.127.79.208	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
109.253.133.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.199.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.2.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-17-2016-18:04:05 to 08-17-2016-19:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.221.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	184
2.53.14.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
2.53.142.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
2.53.45.162	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
46.19.86.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
77.127.2.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.139.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.179.204.44	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-22422	Block	3
176.13.21.98	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.53.48.169	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
66.249.93.107	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.249.78.62	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.62	Block	3
81.131.221.61	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
60.190.60.78	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 60.190.60.78	Block	2
85.250.169.161	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
77.138.67.217	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
2.55.54.151	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.9	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.254	Block	1
60.190.60.78	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.asp	Block	1
37.26.149.245	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
67.245.1.115	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-17128-he/	Block	1
66.249.78.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/7/ שקופית3	Block	1
87.70.247.126	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
46.19.86.96	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
77.138.243.23	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
24.16.121.217	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 24.16.121.217	Block	1
217.132.0.192	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1274-he/atal.aspx	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/apple-app-site-association	Block	1
66.102.9.54	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
109.253.194.122	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
41.40.67.249	Egypt	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
77.126.35.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
180.76.15.146	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list20050529.htm	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI in www.aka.idf.il/chinuch/faq/default.asp	None	1
87.70.247.126	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
24.16.121.217	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/	Block	1
77.138.243.23	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus	Block	1
66.102.9.105	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
41.40.67.249	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
84.111.81.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/894-he/miluim.aspx	Block	1
2.53.56.248	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
192.243.55.131	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcdhphdmltxdc0ns5kb2m=&infocenteritem=true	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.64.137.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.154.81.24	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
79.177.1.48	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.93.111	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.168	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1

08-17-2016-18:04:05 to 08-17-2016-19:04:05