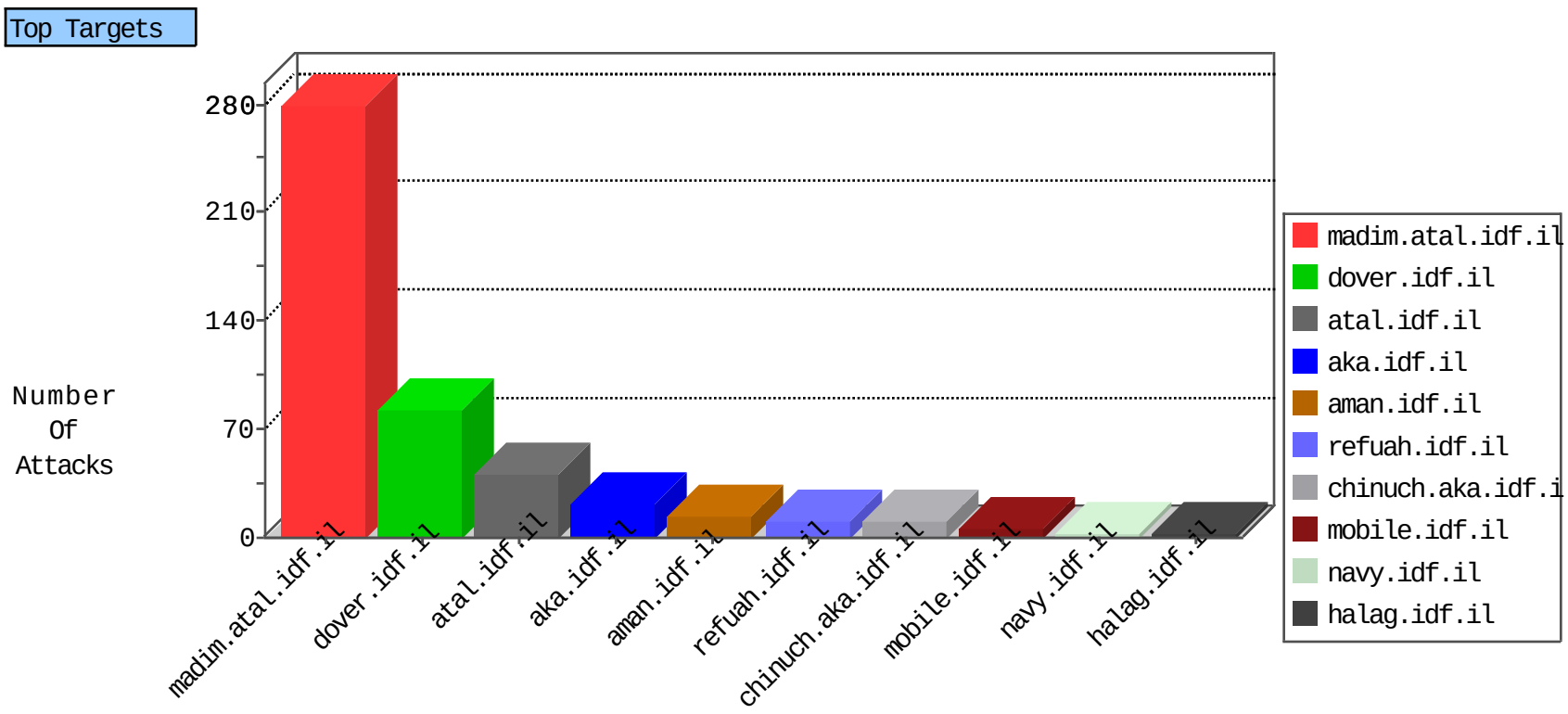
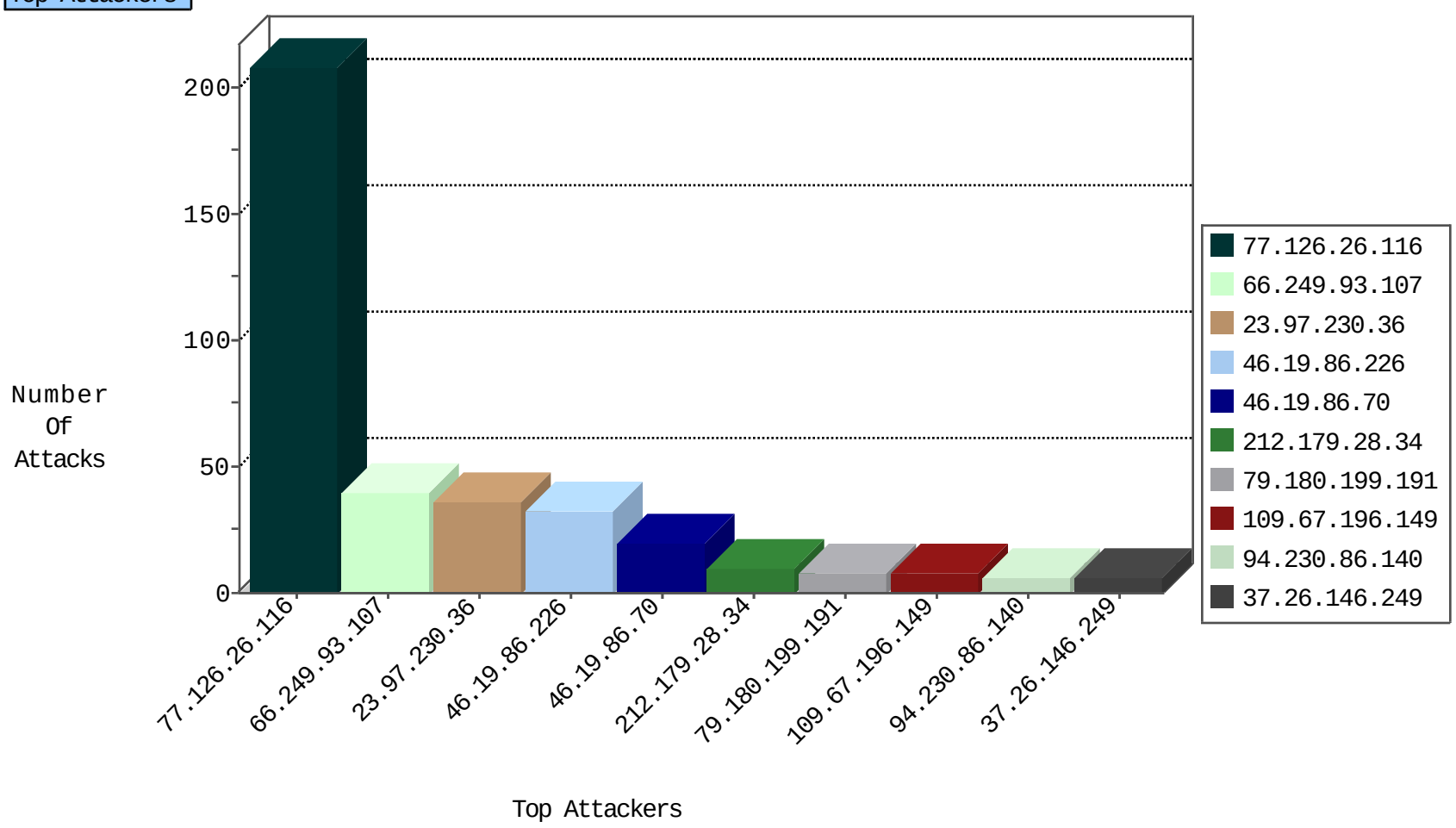
08-20-2016-23:04:03 to 08-21-2016-00:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-20-2016-23:04:03 to 08-21-2016-00:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.76.86	navy.idf.il	Black List	drop	1
91.230.121.156	Ukraine	147.237.76.30	himush.idf.il	Black List	drop	1
123.59.59.52	China	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
37.26.148.170	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
123.59.59.52	China	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1

08-20-2016-23:04:03 to 08-21-2016-00:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.97.230.36	Netherlands	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
23.97.230.36	Netherlands	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	3
23.97.230.36	Netherlands	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	3
51.255.65.7	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
23.97.225.177	Netherlands	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
51.255.65.82	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-20-2016-23:04:03 to 08-21-2016-00:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
23.97.230.36	147.237.77.233	Netherlands	atal.idf.il	SQL Injection - Select From	18
109.67.196.149	147.237.76.42	Israel	refuah.idf.il	ET SCAN NMAP -sA (2)	8
23.97.230.36	147.237.77.233	Netherlands	atal.idf.il	ET WEB_SERVER ATTACKER SQLi - SELECT and Schema Columns	8
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	4
77.124.14.110	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	3
37.143.82.50	147.237.8.24	Netherlands	e.lifestyle.idf.	ET SCAN NMAP -sS window 2048	1
23.97.225.177	147.237.77.233	Netherlands	atal.idf.il	SQL Injection - Select From	1
198.20.69.98	147.237.76.177	United States	ncore.idf.il	ET DROP Dshield Block Listed Source	1
46.172.71.251	147.237.77.234	Ukraine	halag.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.8.24	Netherlands	e.lifestyle.idf.	ET SCAN NMAP -f -sS	1

08-20-2016-23:04:03 to 08-21-2016-00:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.107	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
66.249.93.107	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.179.28.34	Israel	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	10
79.180.199.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
213.151.43.232	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
94.230.86.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.107	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
68.180.228.185	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
31.168.173.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
176.13.16.117	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
84.110.34.203	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
5.102.194.91	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.120.126.4	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
109.253.215.134	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
73.93.142.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.217.62	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.248.193	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1

08-20-2016-23:04:03 to 08-21-2016-00:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.126.26.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	208
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
46.19.86.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
37.142.64.227	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
37.26.146.249	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	3
46.19.85.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.148.191	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.229.2.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.146.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
77.125.22.206	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	3
66.249.65.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.177	Block	2
46.19.86.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.153.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
188.37.159.203	Portugal	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/news.aspx	Block	2
66.102.9.105	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
139.129.130.253	China	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
77.125.22.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/3/	Block	1
46.117.38.140	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
207.46.13.126	United States	147.237.72.166	aka.idf.il	Unknown Parameter c in aka.idf.il/miluim/templates/inner.asp	None	1
78.27.160.157	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
139.129.130.253	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
46.117.213.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
207.46.13.126	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/sachar/faq.aspx	None	1
46.19.85.88	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
79.183.91.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.76.122	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/about/memorial/pages/elhozayeltaleb.aspx	Block	1
157.55.39.174	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/robots.txt	Block	1
77.138.67.217	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
46.120.131.60	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
207.46.13.145	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
46.19.85.88	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method deflate in URL	Block	1
66.249.93.103	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
157.55.39.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/chinuch/news/	None	1
41.34.152.232	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
77.138.226.144	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
46.121.119.177	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
109.64.1.132	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.i	SSL Untraceable Connection - Open Mode	None	1
46.19.85.15	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
78.27.160.157	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 78.27.160.157	Block	1

08-20-2016-23:04:03 to 08-21-2016-00:04:03