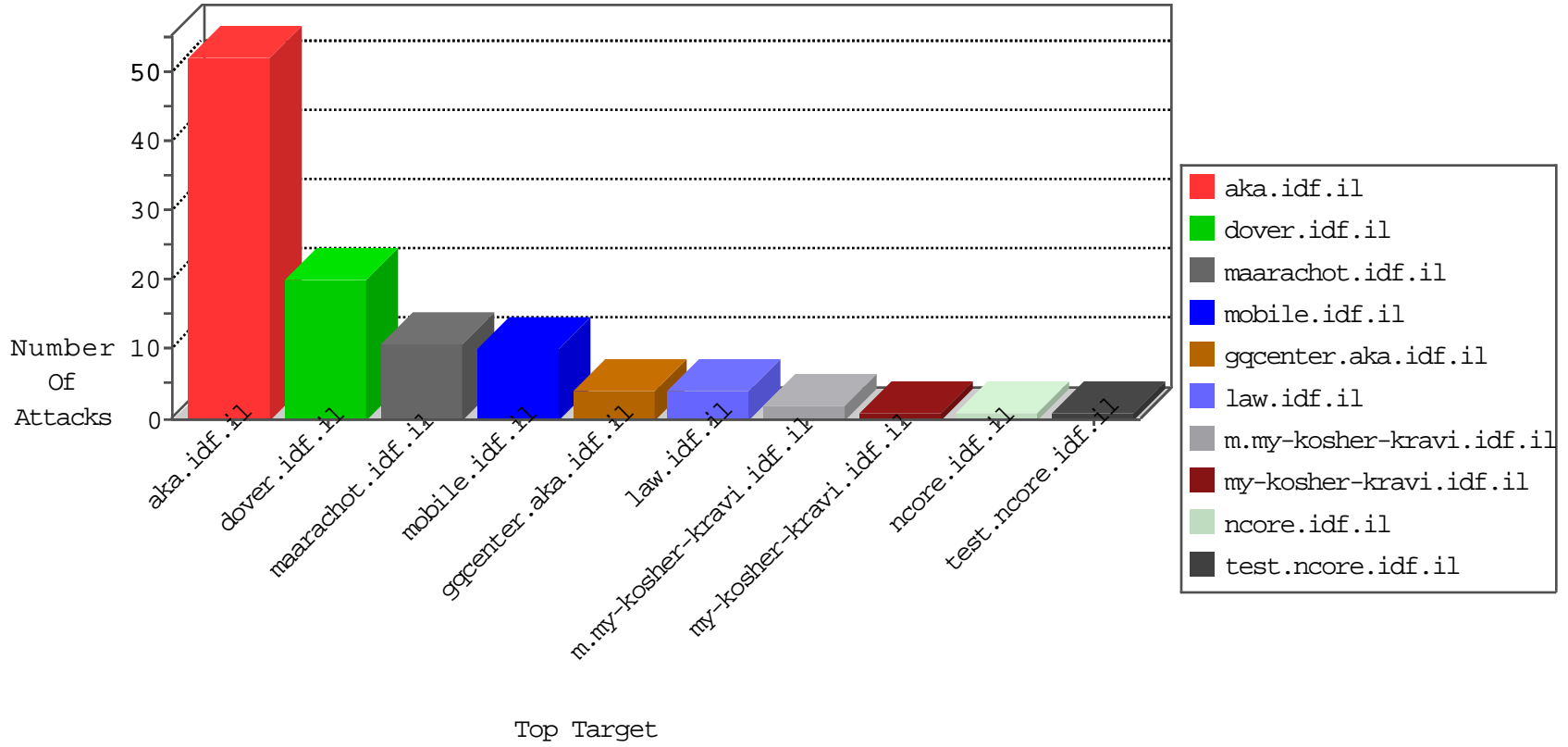


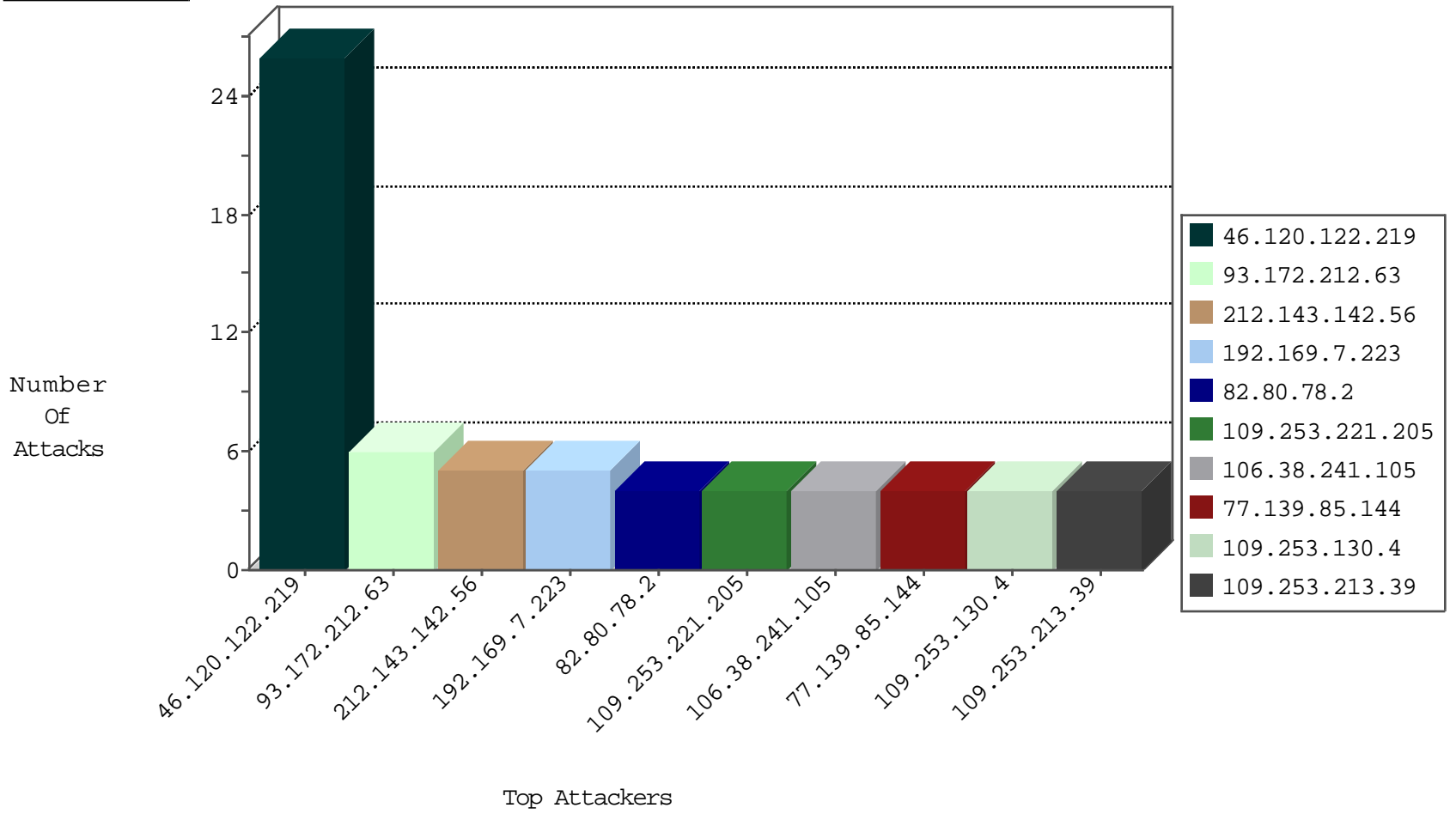
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	4
93.158.200.97	Netherlands	147.237.76.177	ncore.idf.il	Black List	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	4
151.80.158.97	France	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	11
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	8
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
163.172.169.150	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
142.54.191.210	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
120.26.213.39	147.237.76.176	China	test.ncore.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
142.54.191.210	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
142.54.191.210	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -f -sS	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.172.212.63	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
109.253.221.205	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.169.7.223	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	4
109.253.213.39	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	4
176.13.231.27	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
66.249.64.16	Israel	147.237.0.33	idf.il	drop		drop	1
176.13.6.248	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.218.206.82	United States	147.237.0.35	akaws.idf.il	drop		drop	1
109.253.128.56	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.121	e.navy.idf.il	drop	SAM rule	drop	1
218.92.147.79	China	147.237.76.34	yochalan.idf.il	drop		drop	1
185.3.147.204	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.139.85.144	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	4
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.120.122.219	Block	4
109.253.130.4	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	4
24.70.214.181	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	2
77.139.96.80	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/sachar	Block	2
89.237.77.35	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	2
185.27.106.123	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.102.9.13	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
207.46.13.149	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/international_courses.asp	Block	1
92.80.187.30	Romania	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
66.249.76.113	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.113	Block	1
192.169.7.223	United States	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/	Block	1
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.35	Block	1
218.92.147.79	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized HTTP Method	Block	1
66.249.76.113	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
46.120.122.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
207.46.13.109	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.181.103.173	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	1
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/6/10	Block	1
218.92.147.79	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
109.253.219.109	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
68.180.230.47	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
46.121.232.143	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsuneymofet.aspx	None	1
207.46.13.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/form.asp	Block	1
89.237.70.223	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
66.249.76.85	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
185.27.106.123	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
74.74.170.185	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.102.6.30	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
207.46.13.149	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/assetlinks.json	Block	1