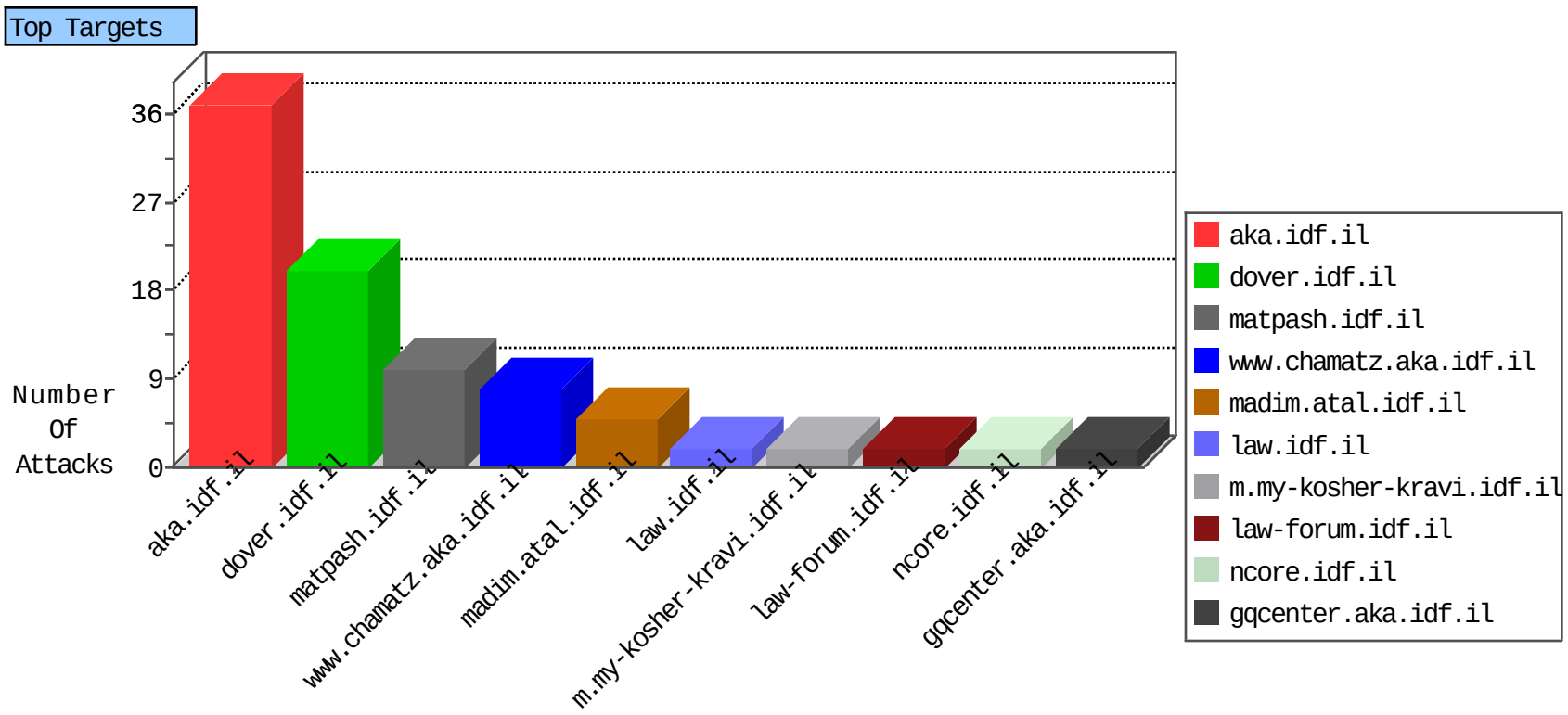
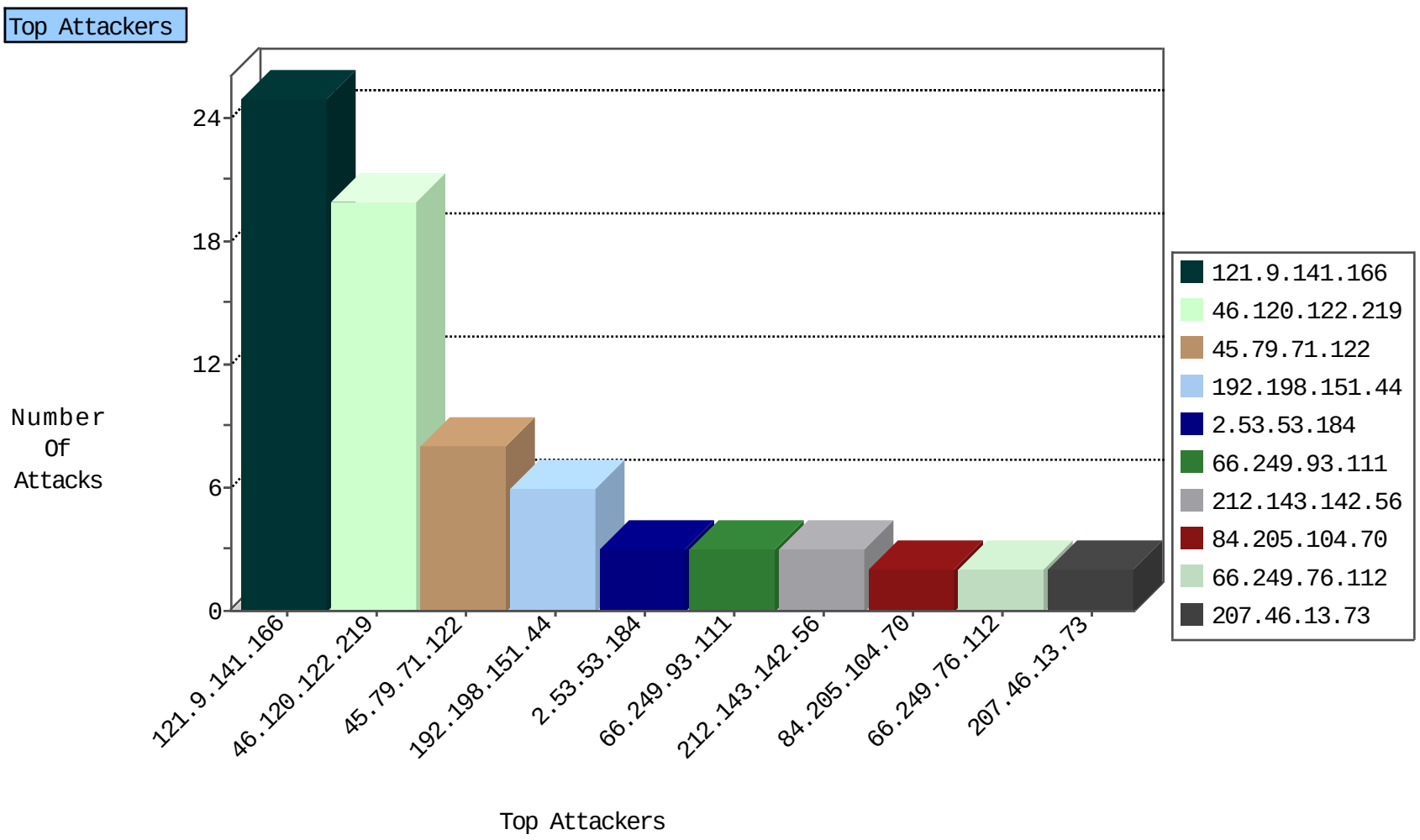
09-04-2016-05:04:04 to 09-04-2016-06:04:04

IDF Under Attack Daily Report





09-04-2016-05:04:04 to 09-04-2016-06:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Black List	drop	2

09-04-2016-05:04:04 to 09-04-2016-06:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-04-2016-05:04:04 to 09-04-2016-06:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.176	Israel	matpash.idf.il	Xenu Link Sleuth User Agent	10
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	8
45.79.71.122	147.237.77.226	United States	www.chamatz.aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	2
87.236.194.161	147.237.0.17	Czech Republic	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
84.205.104.70	147.237.77.19	Egypt	law-forum.idf.il	ET SCAN NMAP -f -sS	1
66.249.64.159	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	1
5.255.90.133	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.76.148	Cote D'Ivoire	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 3072	1
94.102.48.195	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
84.205.104.70	147.237.77.19	Egypt	law-forum.idf.il	ET SCAN NMAP -sS window 2048	1
79.118.133.136	147.237.76.30	Romania	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
5.255.90.133	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.76.148	Cote D'Ivoire	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
177.200.192.50	147.237.0.17	Brazil	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1

09-04-2016-05:04:04 to 09-04-2016-06:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
66.249.93.111	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
200.34.218.70	Brazil	147.237.0.35	akaws.idf.il	drop		drop	1
46.116.77.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

09-04-2016-05:04:04 to 09-04-2016-06:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
121.9.141.166	China	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 121.9.141.166	Block	17
121.9.141.166	China	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
192.198.151.44	Europe	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	5
2.53.53.184	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
45.79.71.122	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unknown HTTP Request Method from 45.79.71.122	Block	2
207.46.13.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
46.19.86.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
45.79.71.122	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Malformed HTTP Header Line from 45.79.71.122	Block	2
45.79.71.122	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Malformed URL from 45.79.71.122	Block	2
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1806-he/dover.aspx	Block	1
121.9.141.166	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/index.asp	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
85.65.192.221	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
136.243.11.18	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.112	Block	1
50.18.94.121	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized Method HEAD for www.chinuch.aka.idf.il/1150-he/chinuch.aspx	None	1
157.55.39.74	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/.well-known/assetlinks.json	Block	1
192.198.151.44	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
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
121.9.141.166	China	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1

09-04-2016-05:04:04 to 09-04-2016-06:04:04