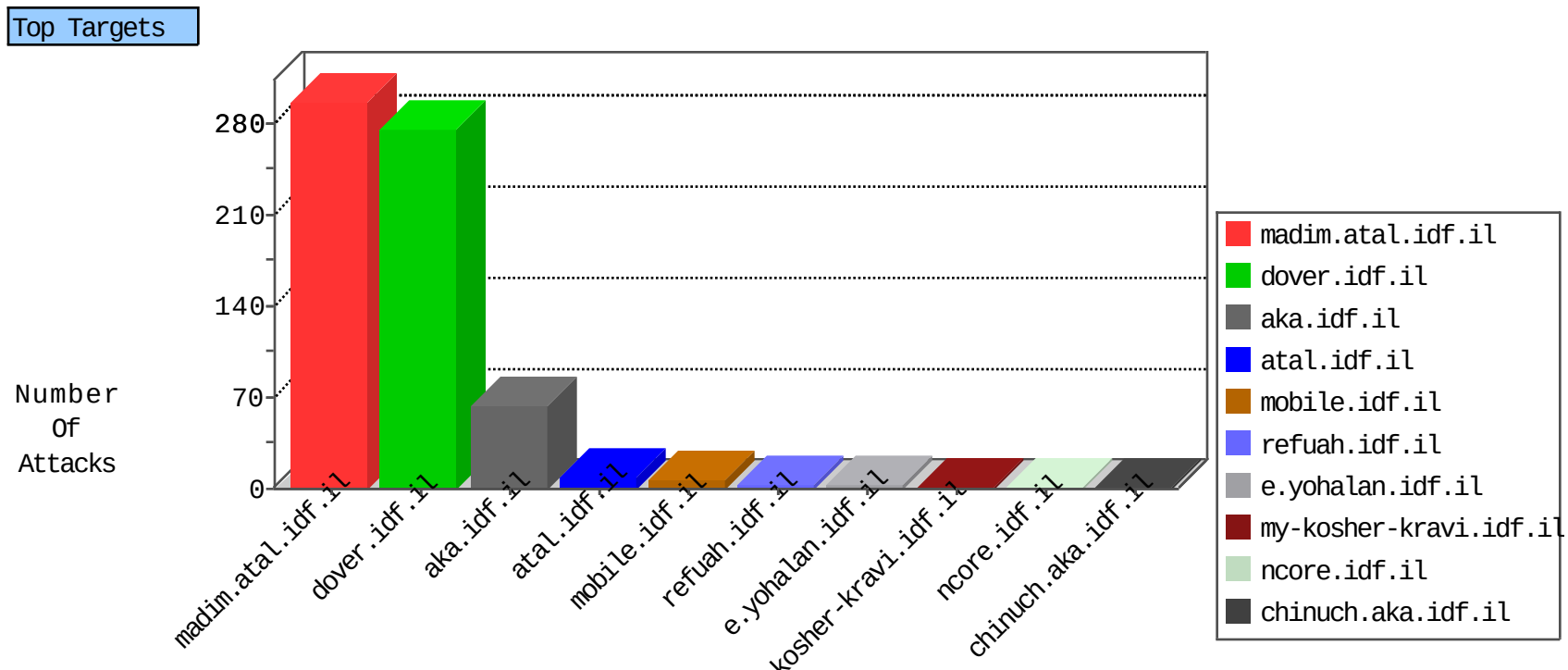
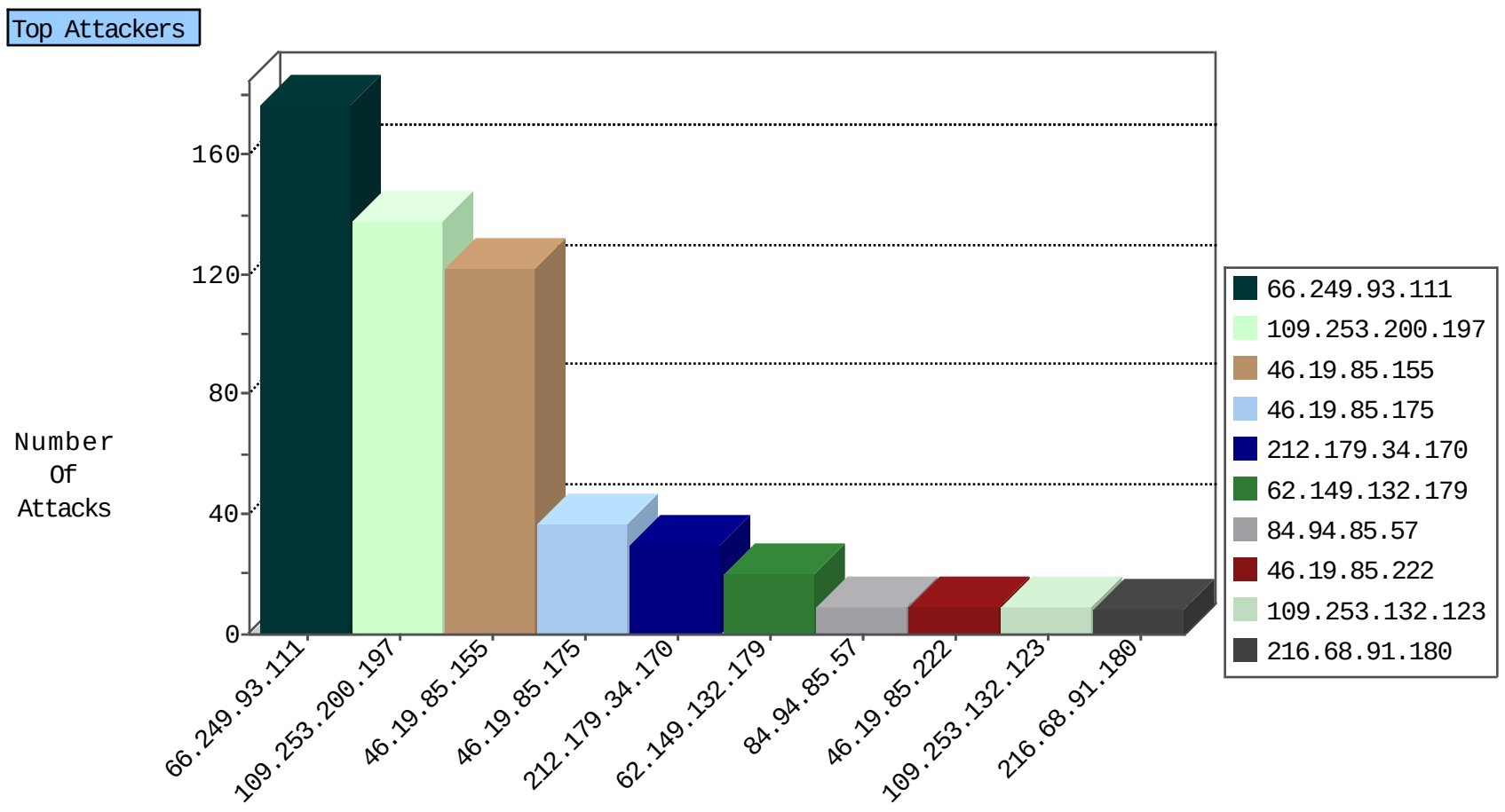
09-04-2016-07:04:00 to 09-04-2016-08:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-04-2016-07:04:00 to 09-04-2016-08:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.19.85.128	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.240.219.146	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

09-04-2016-07:04:00 to 09-04-2016-08:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-04-2016-07:04:00 to 09-04-2016-08:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.149.132.179	147.237.72.166	Italy	aka.idf.il	SQL Injection - Select From	20
216.68.91.180	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	2
208.100.26.228	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.77.212	Canada	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
87.236.194.161	147.237.8.46	Czech Republic	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
64.233.172.135	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
46.227.67.172	147.237.77.19	Sweden	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.138	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
87.236.194.161	147.237.76.177	Czech Republic	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.119	147.237.76.42	Europe	refuah.idf.il	ET SCAN NMAP -sA (2)	1

09-04-2016-07:04:00 to 09-04-2016-08:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	SAM rule	drop	117
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	53
46.19.85.175	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	34
212.179.34.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.239.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.93.111	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
212.76.102.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
64.233.172.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.175	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.117.250.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.231.77	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.147.208.38	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.178.1.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
5.102.242.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
207.46.13.45	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.185	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
80.246.130.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.201	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
213.8.204.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
104.237.234.109	United States	147.237.0.200	m4u.idf.il	drop		drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.105	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
157.55.39.221	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
66.249.69.2	Israel	147.237.0.33	idf.il	drop		drop	1

09-04-2016-07:04:00 to 09-04-2016-08:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.200.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	138
46.19.85.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
46.19.85.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.253.132.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.53.157.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
84.94.85.57	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	4
2.53.7.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.94.85.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.212.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.92.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/undefined	Block	2
84.94.85.57	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
207.46.13.45	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.173.41.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/70288.pdf	Block	1
2.53.26.239	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	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/	Block	1
84.94.85.57	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 84.94.85.57	Block	1
105.156.109.202	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1415-13139-ar/doyoutube to mp3ver.aspx	Block	1
77.138.152.101	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/faq.aspx	Block	1
178.154.149.7	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/null	Block	1
77.139.65.65	France	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx	Block	1
5.29.51.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.115.64.250	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
46.19.86.182	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
192.115.64.250	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	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

09-04-2016-07:04:00 to 09-04-2016-08:04:00