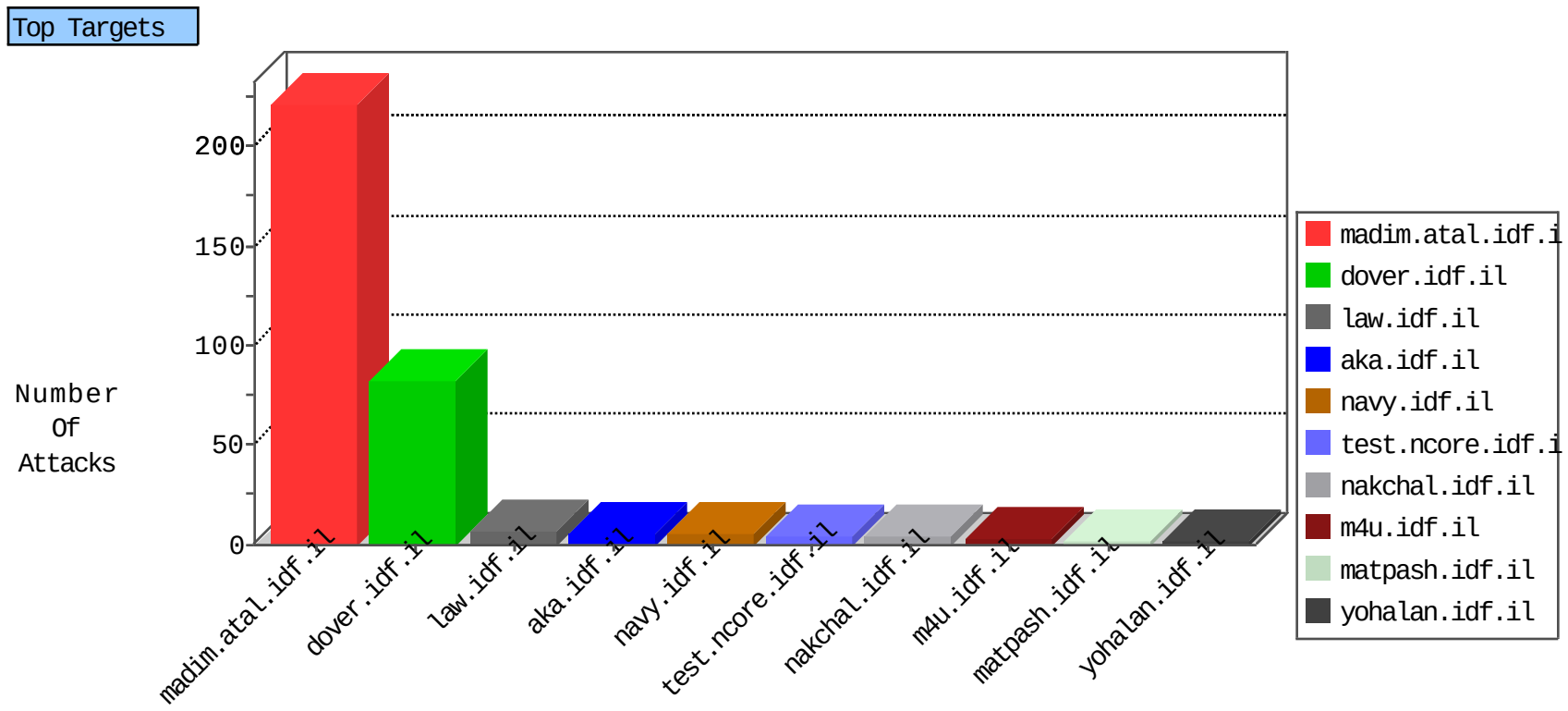
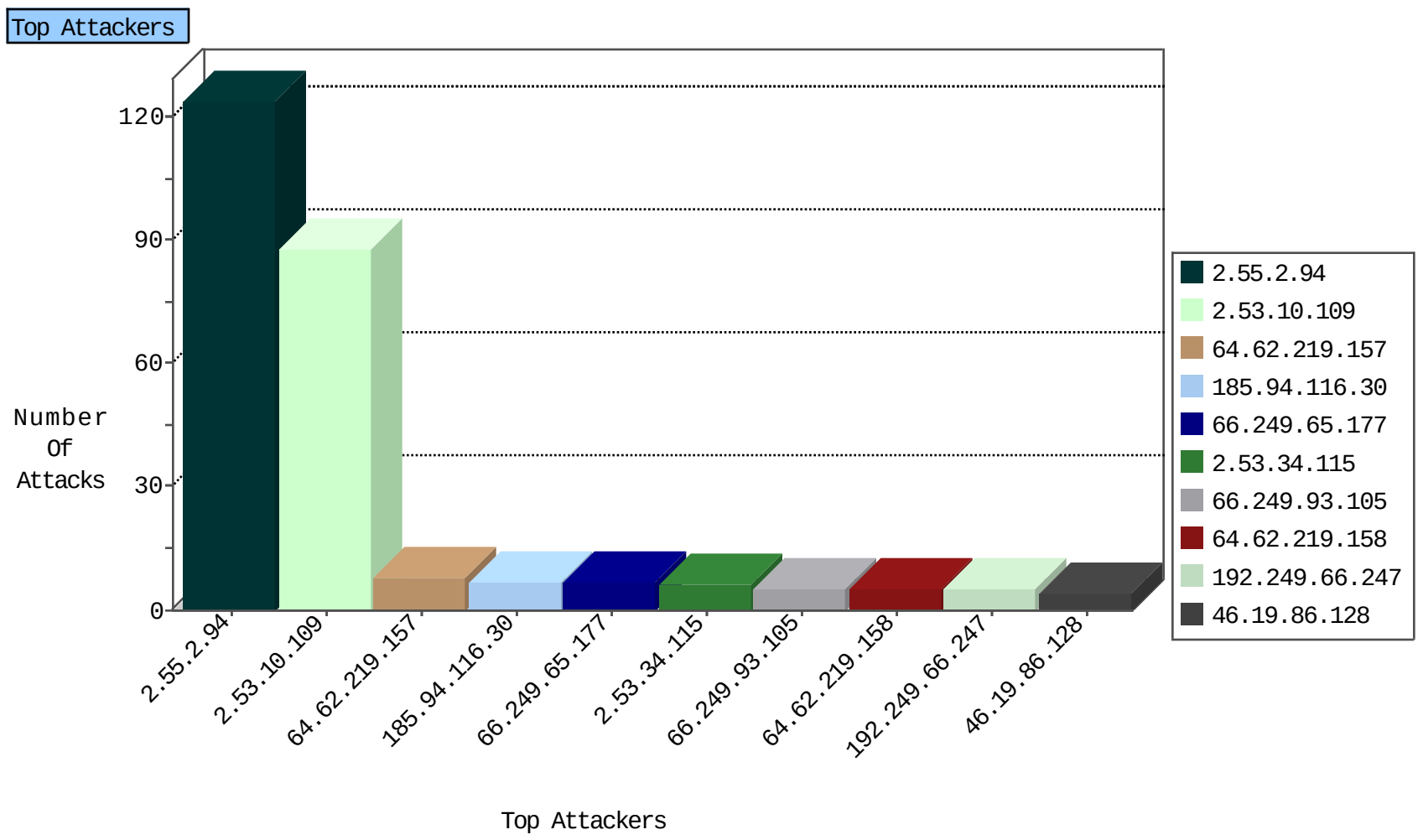
08-21-2016-07:04:09 to 08-21-2016-08:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-21-2016-07:04:09 to 08-21-2016-08:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.178.110.84	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4
192.249.66.247	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
110.13.212.158	Korea, Republic of	147.237.76.34	yohalan.idf.il	Black List	drop	2
216.26.141.7	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
125.64.94.200	China	147.237.76.176	test.ncore.idf.il	Black List	drop	1
216.26.141.6	United States	147.237.77.74	law.idf.il	Invalid TCP Flags	drop	1
125.64.94.200	China	147.237.76.177	ncore.idf.il	Black List	drop	1
216.26.141.6	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
123.59.59.52	China	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
125.64.94.200	China	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
216.26.141.7	United States	147.237.77.74	law.idf.il	Invalid TCP Flags	drop	1
125.64.94.200	China	147.237.76.30	himush.idf.il	Black List	drop	1

08-21-2016-07:04:09 to 08-21-2016-08:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.94.116.30	United Kingdom	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	7
164.132.161.50	Italy	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-21-2016-07:04:09 to 08-21-2016-08:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.105	147.237.76.86	Europe	navy.idf.il	ET SCAN NMAP -sA (2)	5
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	4
54.201.202.214	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
23.94.86.8	147.237.0.19	United States	madim.atal.idf.il	WEB-CGI redirect access	1
129.56.2.38	147.237.76.42	Nigeria	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
54.201.202.214	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
54.201.202.214	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -f -sS	1

08-21-2016-07:04:09 to 08-21-2016-08:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.110.35.144	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
109.253.192.194	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
81.218.70.243	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.110	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
64.62.219.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.134.90	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
36.81.205.41	Indonesia	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.48	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
64.62.219.157	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.226.236	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
71.6.158.166	United States	147.237.0.200	m4u.idf.il	drop		drop	1
184.105.247.248	United States	147.237.0.200	m4u.idf.il	drop		drop	1
74.82.47.31	United States	147.237.0.200	m4u.idf.il	drop		drop	1

08-21-2016-07:04:09 to 08-21-2016-08:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.2.94	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	124
2.53.10.109	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	88
66.249.65.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.177	Block	7
2.53.34.115	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	6
37.26.148.254	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
31.13.102.122	Ireland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/ https:/twitter.com/	Block	1
82.166.244.220	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.128	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method Q5VUP017XQNEKK8TUJERM49H&SessionCode=UP in URL www.idf.ilhttp/1.1	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/0/71090.doc	Block	1
89.138.163.56	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
46.19.86.167	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.128	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
118.92.114.134	New Zealand	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/163-7353-en/patzar.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/2/71562.pdf	Block	1
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.128	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
46.19.86.128	Israel	147.237.77.216	dover.idf.il	Malformed URL http/1.1	Block	1

08-21-2016-07:04:09 to 08-21-2016-08:04:09