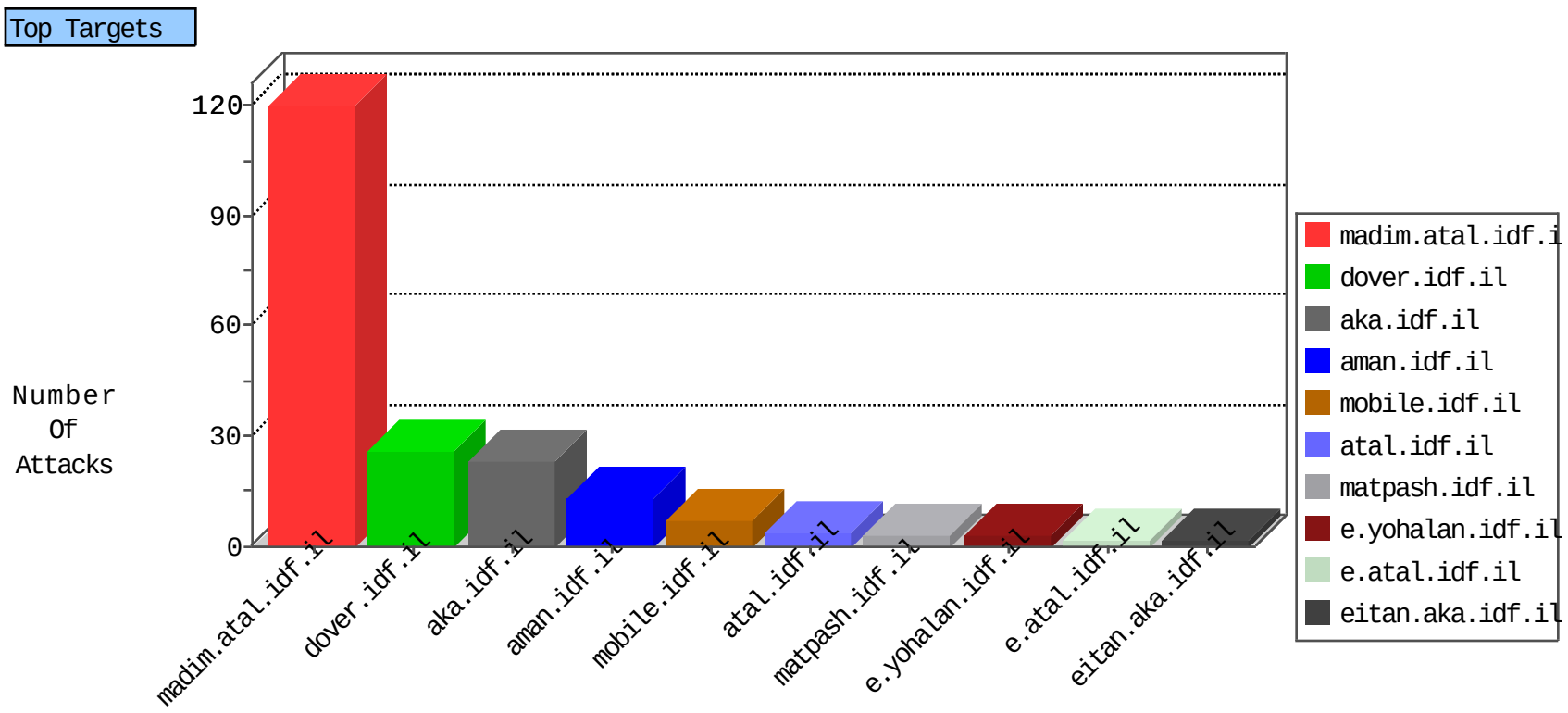
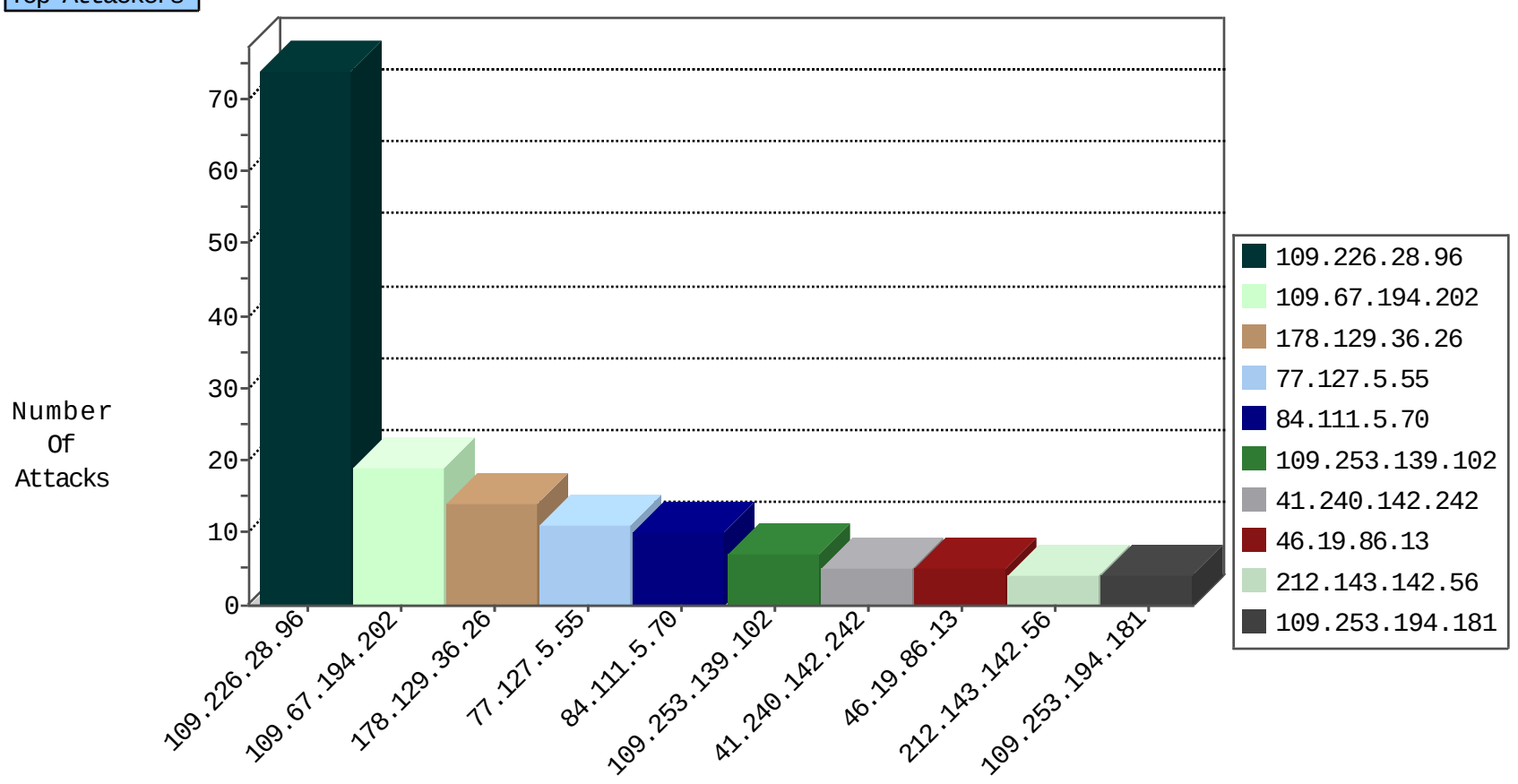
09-02-2016-19:04:08 to 09-02-2016-20:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-02-2016-19:04:08 to 09-02-2016-20:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
134.147.203.115	Germany	147.237.76.198	e.yohalan.idf.il	Black List	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
134.147.203.115	Germany	147.237.76.200	eitan.aka.idf.il	Black List	drop	2
94.156.128.101	Bulgaria	147.237.76.44	e.refuah.idf.il	Black List	drop	1
97.82.197.5	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-02-2016-19:04:08 to 09-02-2016-20:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-02-2016-19:04:08 to 09-02-2016-20:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
178.129.36.26	147.237.76.201	Russian Federation	e.atal.idf.il	ET SCAN Potential SSH Scan	2
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	1
178.129.36.26	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
178.129.36.26	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN Potential SSH Scan	1
178.129.36.26	147.237.76.199	Russian Federation	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
178.129.36.26	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
178.129.36.26	147.237.72.217	Russian Federation	e.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.76.198	Canada	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.138	147.237.77.212	Ukraine	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	1
178.129.36.26	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN Potential SSH Scan	1
54.166.76.158	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
178.129.36.26	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
178.129.36.26	147.237.77.170	Russian Federation	maarachot.idf.il	ET SCAN Potential SSH Scan	1
178.129.36.26	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential SSH Scan	1
178.129.36.26	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Potential SSH Scan	1
221.204.249.157	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
178.129.36.26	147.237.72.156	Russian Federation	aman.idf.il	ET SCAN Potential SSH Scan	1
193.201.225.138	147.237.77.233	Ukraine	atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.160.106	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
191.109.95.67	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.224.160.106	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	1
178.129.36.26	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN Potential SSH Scan	1

09-02-2016-19:04:08 to 09-02-2016-20:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.127.5.55	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	11
109.253.139.102	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
41.240.142.242	Sudan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.13	Israel	147.237.72.166	aka.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	4
109.253.135.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
87.115.137.146	United Kingdom	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
93.80.51.106	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
95.28.59.25	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.139.93.40	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.35	akaws.idf.il	drop		drop	1
125.77.28.26	China	147.237.0.35	akaws.idf.il	drop		drop	1
125.77.28.26	China	147.237.76.34	yohalan.idf.il	drop		drop	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

09-02-2016-19:04:08 to 09-02-2016-20:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.226.28.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	74
109.67.194.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
84.111.5.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
109.253.194.181	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.149.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.148.161	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.149.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
87.68.40.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.148.176	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.32.179.99	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.120.50.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.149.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/miluim/templates/inner.asp	Block	1
85.64.148.245	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.69.215	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/19102010hilulatrachel.aspx	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	1
157.55.39.173	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.76.2	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/apple-app-site-association	Block	1
79.178.194.232	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
109.65.110.240	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
37.26.148.176	Israel	147.237.77.243	mobile.idf.il	Suspicious Response Code	Block	1
109.253.194.181	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
80.246.137.20	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
204.79.180.19	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
109.65.110.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/contact/contact.asp	Block	1
136.243.11.18	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.117	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17753-he/dover.aspx	Block	1

09-02-2016-19:04:08 to 09-02-2016-20:04:08