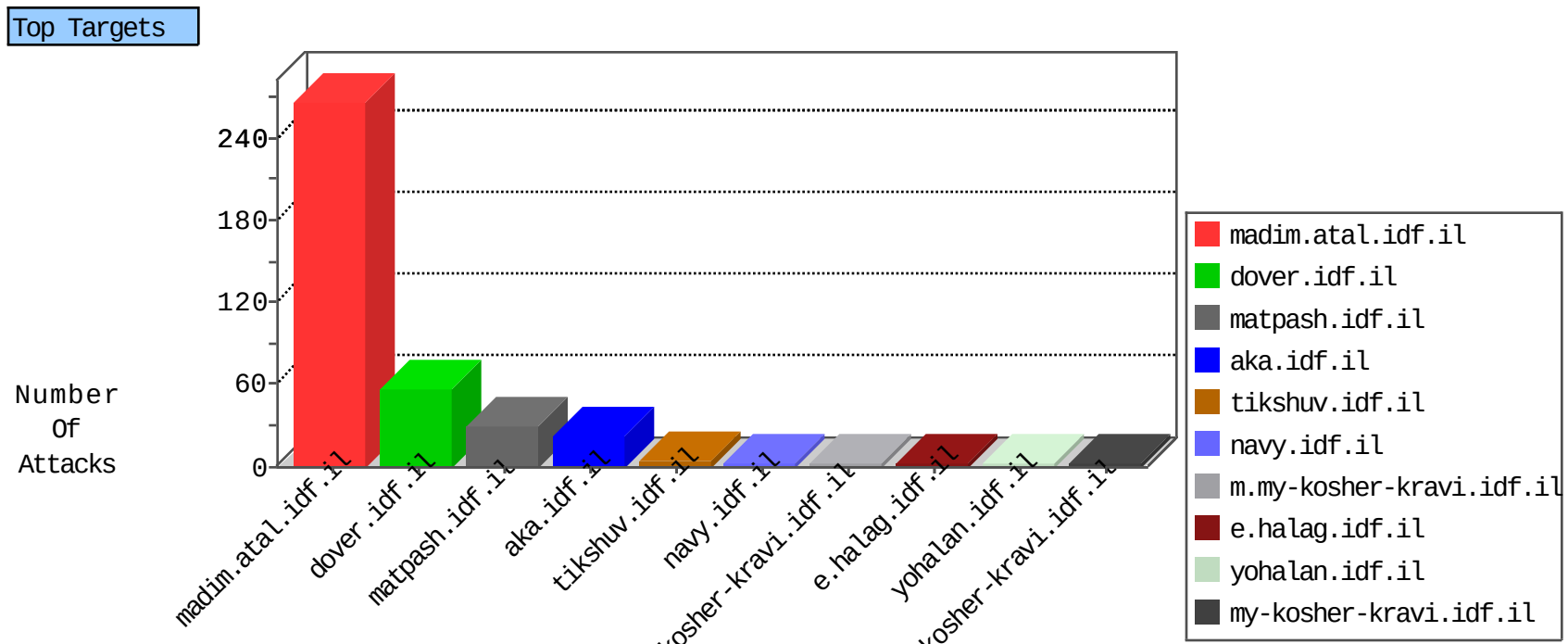
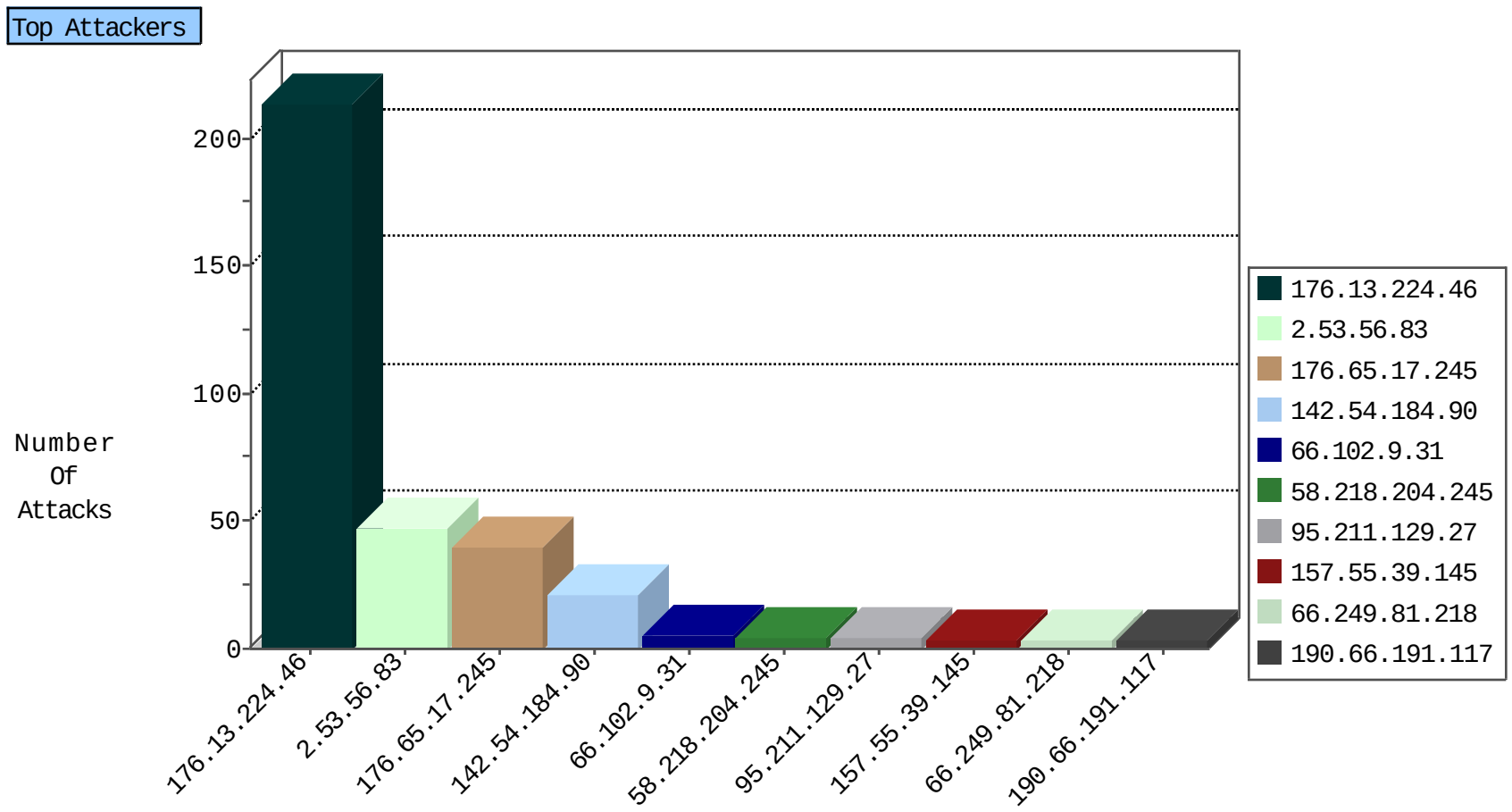
08-19-2016-23:04:02 to 08-20-2016-00:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-19-2016-23:04:02 to 08-20-2016-00:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.155.34	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
190.66.191.117	Colombia	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
123.59.59.52	China	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	1
104.148.55.162	United States	147.237.76.44	e.refuah.idf.il	Black List	drop	1
139.162.13.205	Singapore	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
113.17.184.25	China	147.237.76.34	yohalan.idf.il	Black List	drop	1
164.132.201.35	Italy	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
113.17.184.25	China	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1

08-19-2016-23:04:02 to 08-20-2016-00:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
142.54.184.90	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	13
142.54.184.90	United States	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Permit	5
142.54.184.90	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
108.59.8.80	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
46.165.197.141	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
66.240.219.146	United States	147.237.0.17	m.my-kosher-kravi.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
5.135.167.84	France	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-19-2016-23:04:02 to 08-20-2016-00:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
54.218.93.102	147.237.77.216	United States	dover.idf.il	Xenu Link Sleuth User Agent	2
190.66.191.117	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
95.211.129.27	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1
95.211.129.27	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
185.93.185.235	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
95.211.129.27	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential SSH Scan	1
95.211.129.27	147.237.8.45	Netherlands	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1

08-19-2016-23:04:02 to 08-20-2016-00:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.65.17.245	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	26
176.65.17.245	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.102.9.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.178.2.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
84.108.187.245	Israel	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
216.243.31.2	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
200.0.33.82	Brazil	147.237.0.200	m4u.idf.il	drop		drop	1
109.253.192.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
212.143.142.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.202.144	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
66.102.9.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-19-2016-23:04:02 to 08-20-2016-00:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.224.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	214
2.53.56.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
66.249.81.218	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
66.102.9.20	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
157.55.39.145	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	3
178.135.117.147	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
178.135.117.132	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.127.13.109	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.123	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	2
2.53.179.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.77.5.58	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/pniot.aspx	Block	1
65.92.185.38	Canada	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 65.92.185.38	Block	1
178.135.117.139	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
82.166.69.222	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
66.249.64.148	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
178.135.117.130	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
75.27.57.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
65.92.185.38	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1
89.237.69.106	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21070-he/idfgdover.aspx	Block	1
178.135.117.136	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.138.136.212	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
66.102.9.42	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
178.135.117.137	Lebanon	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.139.241.56	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	1
66.102.9.43	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1

08-19-2016-23:04:02 to 08-20-2016-00:04:02