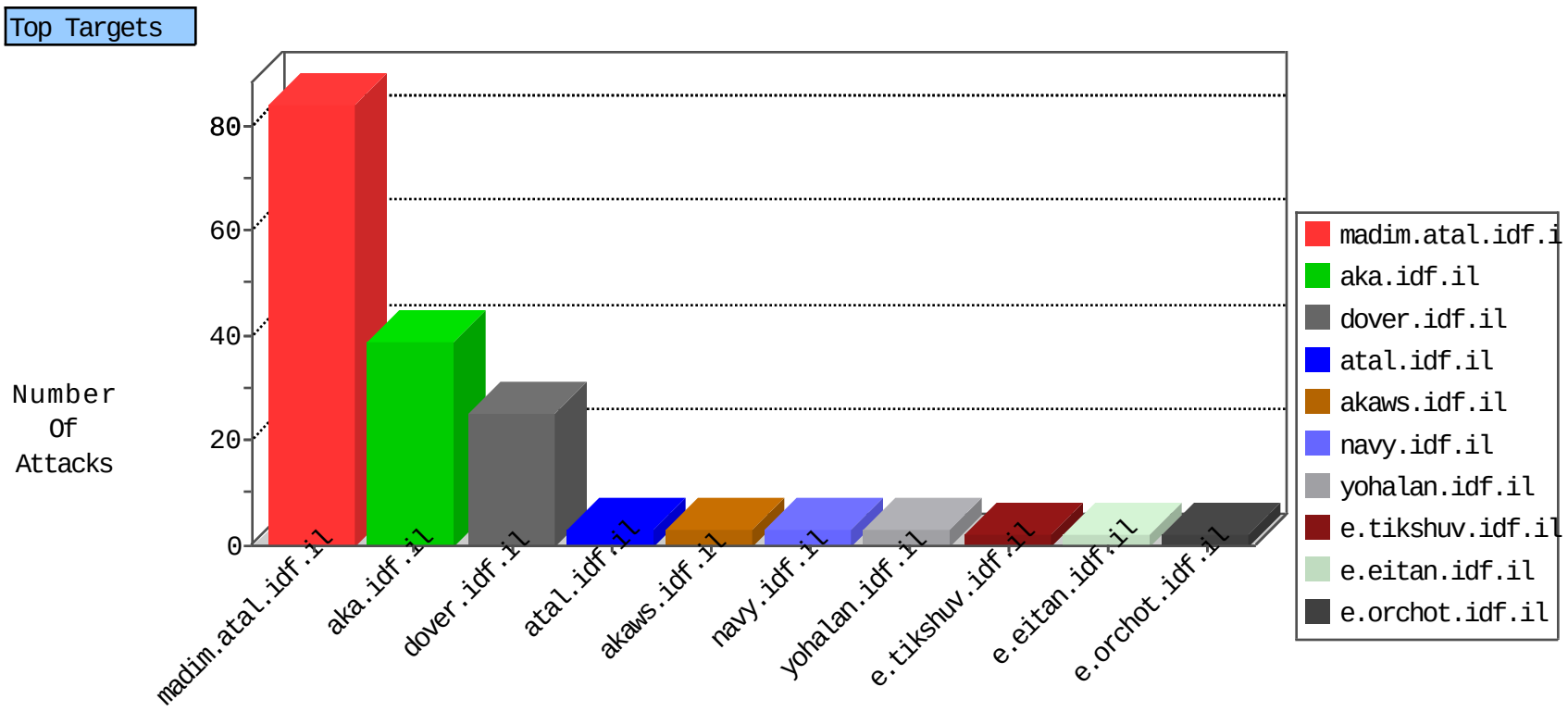
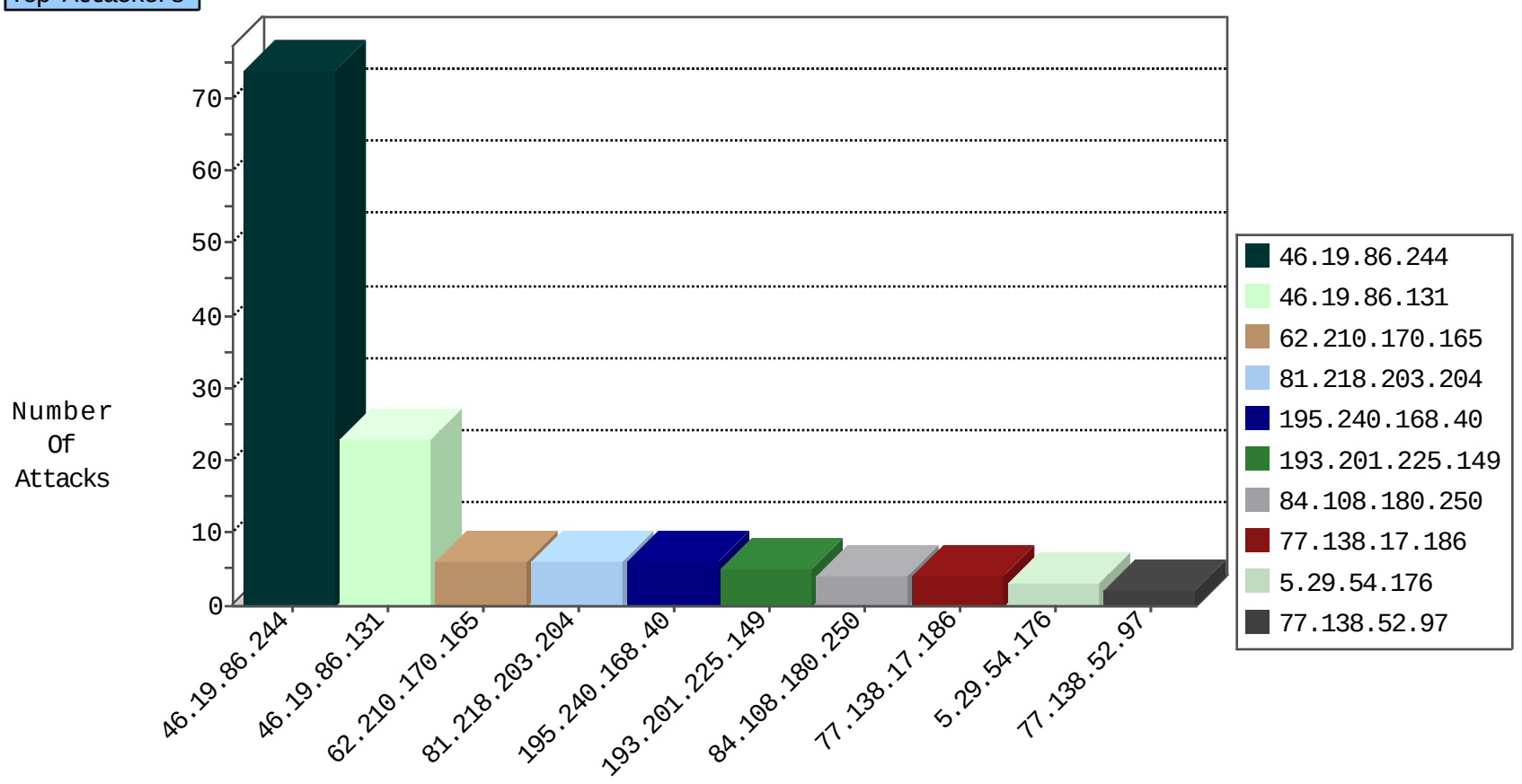
08-19-2016-20:04:04 to 08-19-2016-21:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-19-2016-20:04:04 to 08-19-2016-21:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
120.132.50.135	China	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
71.6.135.131	United States	147.237.76.177	ncore.idf.il	Black List	drop	1
179.32.235.199	Colombia	147.237.77.235	sviva.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
208.67.1.29	United States	147.237.76.42	refuah.idf.il	Black List	drop	1

08-19-2016-20:04:04 to 08-19-2016-21:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.170.165	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	4
62.210.170.165	France	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
5.189.144.121	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	10993: HTTP: Morfeus Scanner Scanning Attempt	Block	1
5.189.144.121	Germany	147.237.0.34	tikshuv.idf.il	10993: HTTP: Morfeus Scanner Scanning Attempt	Block	1

08-19-2016-20:04:04 to 08-19-2016-21:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
81.218.203.204	147.237.77.216	Israel	dover.idf.il	ET SCAN NMAP -sA (2)	6
54.218.93.102	147.237.72.166	United States	aka.idf.il	Xenu Link Sleuth User Agent	2
193.201.225.149	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
179.32.235.199	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
117.27.240.24	147.237.8.45	China	e.eitan.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
193.201.225.149	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.149	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
183.129.160.229	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
139.162.13.205	147.237.77.121	Singapore	e.navy.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
87.68.6.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.205.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.225.149	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
193.201.225.149	147.237.8.46	Ukraine	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1

08-19-2016-20:04:04 to 08-19-2016-21:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.86.131	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
195.240.168.40	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.120.228.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.54	United States	147.237.0.35	akaws.idf.il	drop		drop	1
216.243.31.2	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.54	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
46.117.182.13	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
109.253.132.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.55	United States	147.237.0.35	akaws.idf.il	drop		drop	1
109.253.214.49	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.53	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
62.219.139.136	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1

08-19-2016-20:04:04 to 08-19-2016-21:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.244	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	59
46.19.86.244	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
77.138.17.186	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	4
84.108.180.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.149.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
5.29.54.176	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
217.186.105.80	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
164.58.14.194	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.79.170	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/shared/ajax/setivgallerycontrol.aspx	Block	1
5.29.54.176	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in atal.idf.il/1440-he/atal.aspx	Block	1
84.108.180.250	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	1
62.219.139.136	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
190.237.253.225	Peru	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.79.176	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/shared/ajax/setivgallerycontrol.aspx	Block	1
104.214.113.139	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.102.9.85	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
204.79.180.217	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
131.253.25.177	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 208.115.111.73	Block	1
79.178.34.87	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.9	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/chinuch/	Block	1
66.249.76.33	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1

08-19-2016-20:04:04 to 08-19-2016-21:04:04