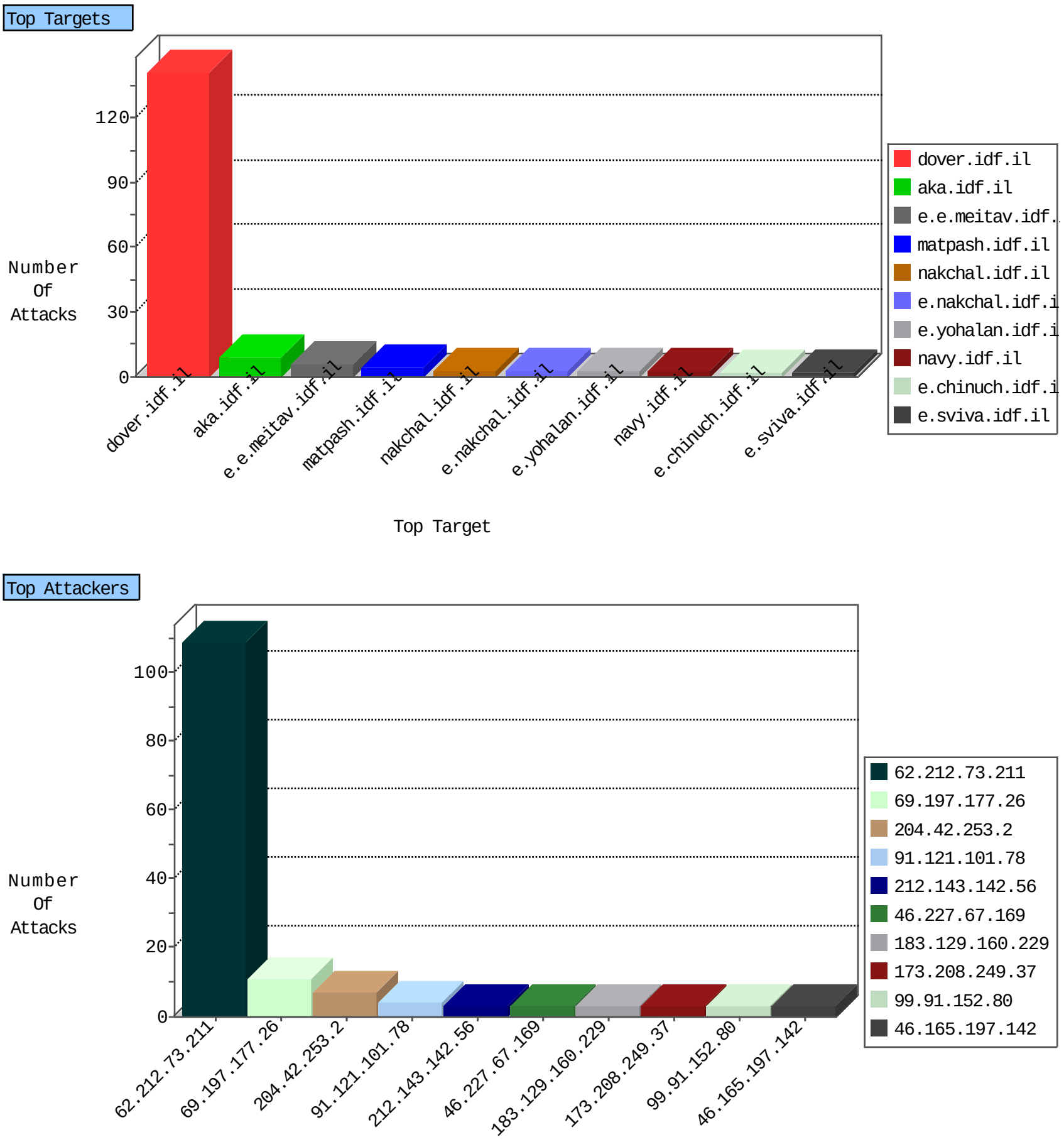
08-19-2016-04:04:02 to 08-19-2016-05:04:02

IDF Under Attack Daily Report



08-19-2016-04:04:02 to 08-19-2016-05:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
222.186.51.181	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Black List	drop	2
180.97.239.31	China	147.237.76.38	e.e.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	2
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Black List	drop	2
202.181.24.48	Hong Kong	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	2
179.33.95.241	Colombia	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
180.97.239.31	China	147.237.76.38	e.e.meitav.idf.il	JLM_Purple_Con_Limit_Http	drop	1
204.42.253.2	United States	147.237.76.30	himush.idf.il	Black List	drop	1

08-19-2016-04:04:02 to 08-19-2016-05:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	107
69.197.177.26	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	11
91.121.101.78	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
46.165.197.142	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	3
62.212.73.211	Netherlands	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
62.210.37.82	France	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

08-19-2016-04:04:02 to 08-19-2016-05:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
173.208.249.37	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
173.208.249.37	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
93.174.91.29	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
85.244.226.214	147.237.8.46	Portugal	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
61.245.177.12	147.237.0.19	Korea, Republic of	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.227.67.169	147.237.77.226	Sweden	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.169	147.237.77.170	Sweden	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
173.208.249.37	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
85.244.226.214	147.237.8.46	Portugal	e.chinuch.idf.il	ET SCAN NMAP -sS window 3072	1
77.28.156.98	147.237.8.27	Macedonia, the Former Yugoslav Republic of	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
54.153.99.128	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.169	147.237.77.178	Sweden	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1

08-19-2016-04:04:02 to 08-19-2016-05:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
99.91.152.80	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
183.129.160.229	China	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.77.243	mobile.idf.il	drop	SAM rule	drop	1
212.143.142.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.212	e.dover.idf.il	drop	SAM rule	drop	1

08-19-2016-04:04:02 to 08-19-2016-05:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	2
207.46.13.145	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.79.157	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/navmenu/	Block	1
66.249.64.176	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/01022011tutim.aspx	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/assetlinks.json	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	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
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/default.aspx	Block	1
66.249.76.39	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.39	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.64.185	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
104.128.144.131	Canada	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/redirect.php	Block	1
66.249.76.39	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/apple-app-site-association	Block	1
64.62.219.80	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
71.197.213.21	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
66.249.66.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/.well-known/assetlinks.json	Block	1
157.55.39.125	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1
66.249.76.52	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.52	Block	1
64.62.219.87	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
73.106.77.179	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1

08-19-2016-04:04:02 to 08-19-2016-05:04:02