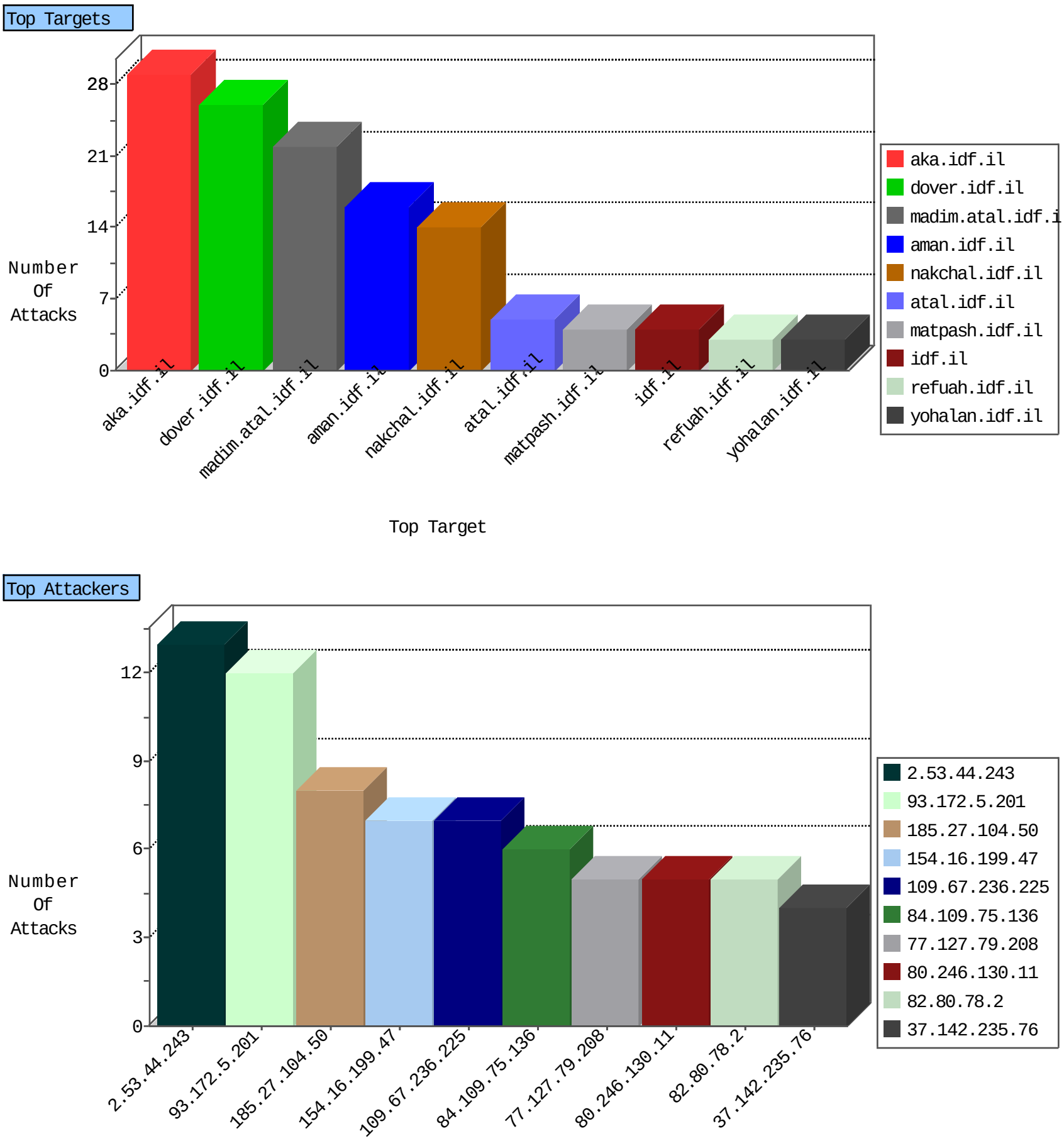
08-17-2016-19:04:07 to 08-17-2016-20:04:07

IDF Under Attack
Daily Report



08-17-2016-19:04:07 to 08-17-2016-20:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.22.131.51	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
82.80.78.2	Israel	147.237.76.86	navy.idf.il	Black List	drop	2
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	2
89.248.171.2	Netherlands	147.237.76.197	e.himush.idf.il	Black List	drop	1
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	1

08-17-2016-19:04:07 to 08-17-2016-20:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.162.163	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2

08-17-2016-19:04:07 to 08-17-2016-20:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.11	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
154.16.199.47	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
154.16.199.47	147.237.72.217	United States	e.idf.il	ET SCAN Potential SSH Scan	1
103.227.193.14	147.237.0.19	Hong Kong	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
87.69.12.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
70.182.176.174	147.237.0.33	United States	idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
154.16.199.47	147.237.77.243	United States	mobile.idf.il	ET SCAN Potential SSH Scan	1
154.16.199.47	147.237.77.19	United States	law-forum.idf.il	ET SCAN Potential SSH Scan	1
154.16.199.47	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
154.16.199.47	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
91.125.184.101	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1
66.249.76.52	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
186.112.108.214	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
154.16.199.47	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1

08-17-2016-19:04:07 to 08-17-2016-20:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
93.172.5.201	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.67.236.225	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
77.127.79.208	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
176.13.14.49	Israel	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
144.76.30.236	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
84.94.221.128	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
144.76.30.236	Germany	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
87.71.20.88	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
195.154.102.122	France	147.237.0.33	idf.il	drop		drop	1
109.253.220.237	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
195.154.102.122	France	147.237.76.34	yohalan.idf.il	drop		drop	1
130.180.216.68	Ukraine	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.178	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.153	United States	147.237.0.33	idf.il	drop		drop	1
176.13.225.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.139.188	Israel	147.237.0.19	madim.atal.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
141.212.122.154	United States	147.237.0.33	idf.il	drop		drop	1
176.13.229.252	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
109.253.213.105	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1

08-17-2016-19:04:07 to 08-17-2016-20:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.44.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
37.142.235.76	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	4
185.27.104.50	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	4
84.109.75.136	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	4
46.19.85.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.27.104.50	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 185.27.104.50	Block	3
2.53.30.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
192.243.55.132	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
109.65.148.243	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
77.138.226.144	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
66.222.239.96	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/forms.aspx	Block	1
2.53.31.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
72.9.148.10	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 72.9.148.10	Block	1
197.48.234.233	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
37.222.213.107	Spain	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/general/	Block	1
139.162.13.205	Singapore	147.237.0.15	kosher-kravi.idf.i	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
77.138.248.30	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx	Block	1
66.249.76.51	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
185.27.104.50	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
84.109.75.136	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 84.109.75.136	Block	1
72.9.148.10	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/kapatz/	Block	1
199.76.44.201	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
139.162.13.205	Singapore	147.237.0.34	tikshuv.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.179.29.245	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/0/	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/sites/skira/default.asp	None	1
185.120.126.29	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
2.84.248.50	Greece	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/drushim	Block	1
84.109.75.136	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/4/	Block	1
77.138.88.199	France	147.237.72.166	aka.idf.il	Post Request - Missing Content Type	Block	1
66.102.9.54	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/kapatz/	Block	1
207.10.18.162	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
148.251.176.212	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
80.246.130.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
192.243.55.129	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
4.16.104.43	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
84.110.209.57	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
77.138.157.248	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.102.9.95	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/	Block	1
84.108.175.124	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1

08-17-2016-19:04:07 to 08-17-2016-20:04:07