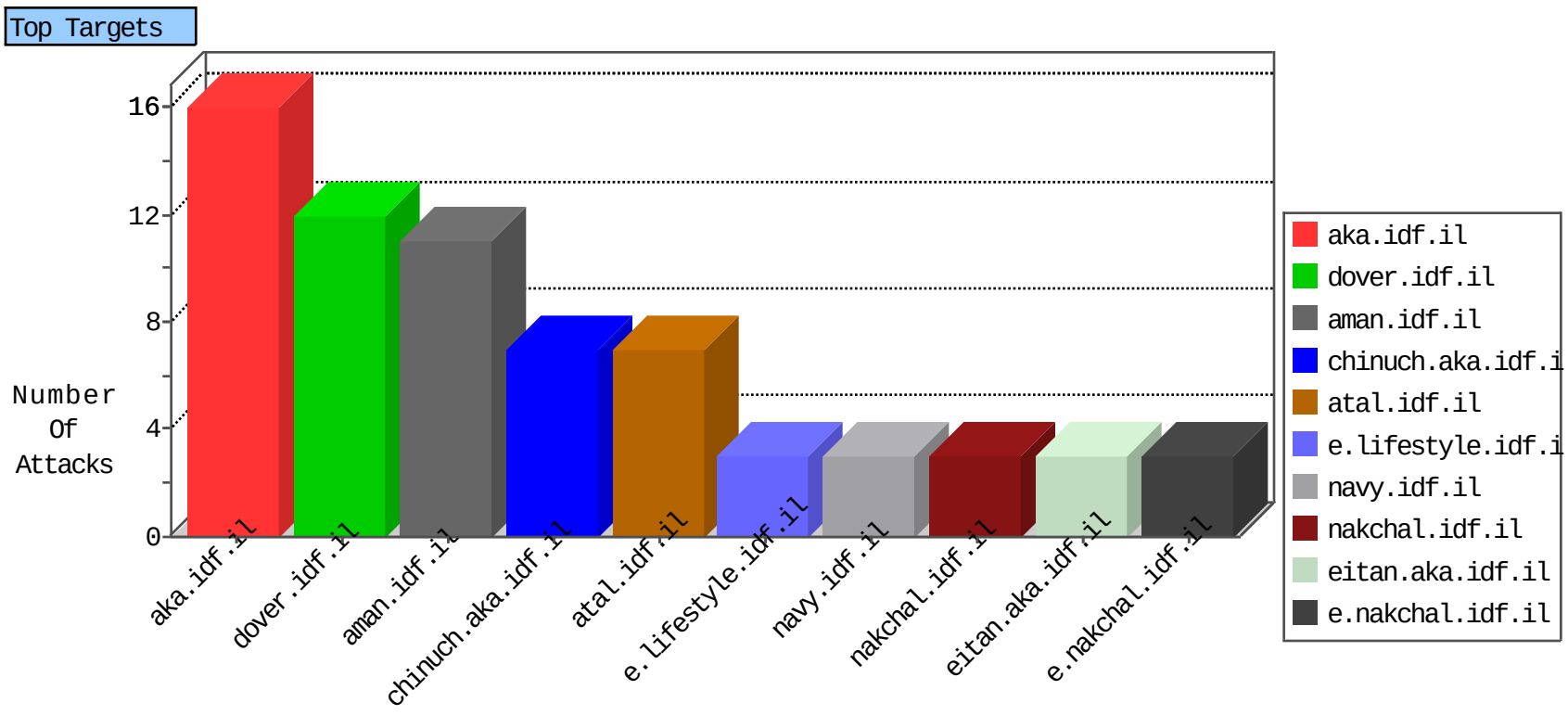
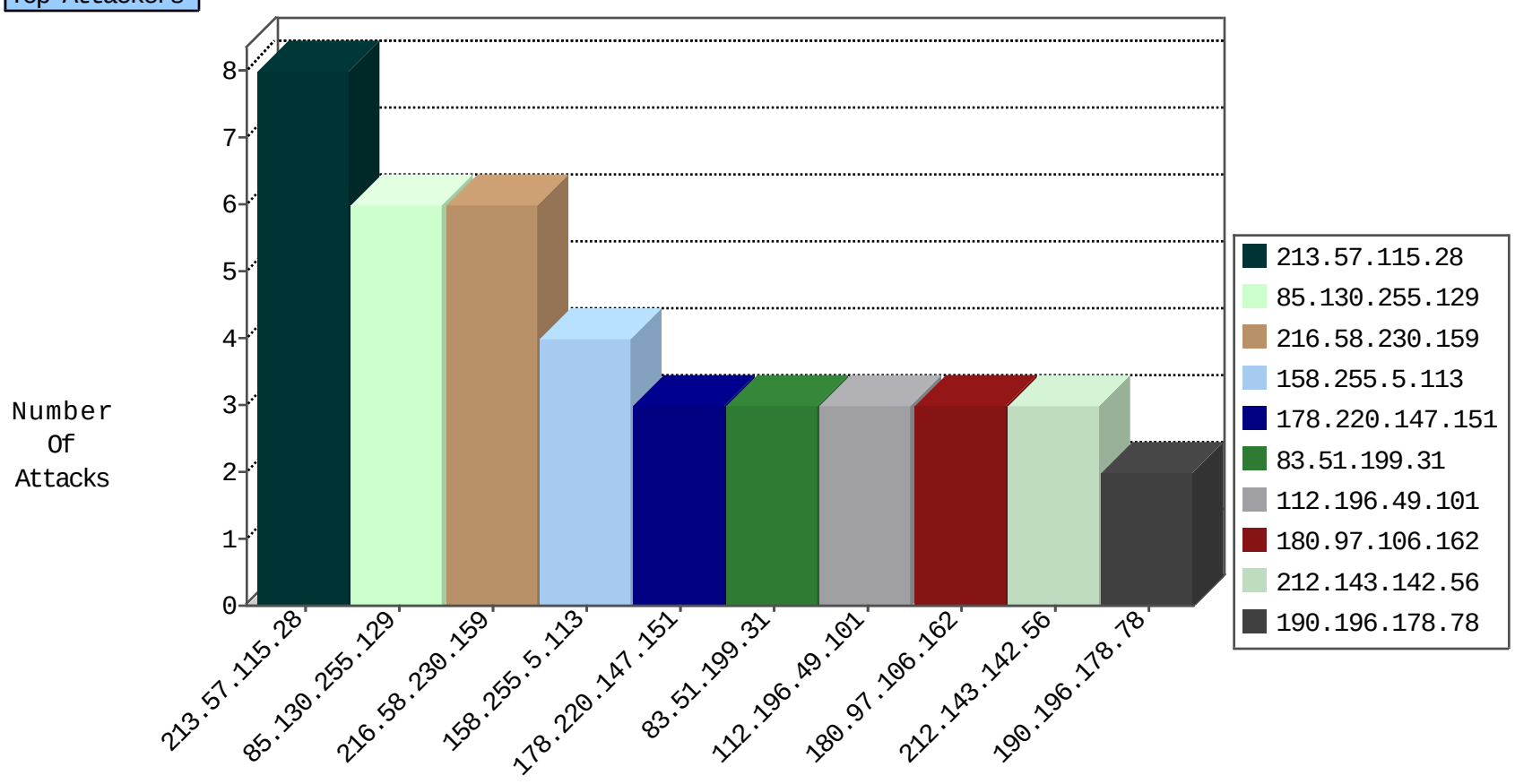
08-17-2016-02:04:09 to 08-17-2016-03:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-17-2016-02:04:09 to 08-17-2016-03:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
154.16.199.174	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
93.158.200.96	Netherlands	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
93.158.200.118	Netherlands	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
93.158.200.132	Netherlands	147.237.76.199	e.nakchal.idf.il	Black List	drop	1

08-17-2016-02:04:09 to 08-17-2016-03:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
88.198.16.153	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
198.20.69.74	United States	147.237.76.201	e.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
216.58.230.159	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

08-17-2016-02:04:09 to 08-17-2016-03:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
216.58.230.159	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	4
109.235.254.181	147.237.76.198	Turkey	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
190.196.178.78	147.237.72.166	Chile	aka.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.158	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
190.79.146.130	147.237.76.31	Venezuela	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.188.131.43	147.237.76.196	Turkey	e.sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
178.220.147.151	147.237.76.200		eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
42.113.139.11	147.237.0.17	Vietnam	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
178.220.147.151	147.237.76.200		eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
158.255.5.113	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1
158.255.5.113	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
112.196.49.101	147.237.8.24	India	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
112.196.49.101	147.237.8.24	India	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.158	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
190.196.178.78	147.237.72.166	Chile	aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.125.184.101	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.29.11.182	147.237.77.74	Latvia	law.idf.il	ET SCAN Potential SSH Scan	1
52.77.57.205	147.237.76.86	Singapore	navy.idf.il	ET SCAN NMAP -sS window 1024	1
178.220.147.151	147.237.76.200		eitan.aka.idf.il	ET SCAN NMAP -sS window 2048	1
158.255.5.113	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
158.255.5.113	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
113.108.10.31	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
112.196.49.101	147.237.8.24	India	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1

08-17-2016-02:04:09 to 08-17-2016-03:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.57.115.28	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	8
85.130.255.129	Israel	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	6
83.51.199.31	Spain	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
180.97.106.161	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
191.96.249.18	Chile	147.237.0.35	akaws.idf.il	drop		drop	1
180.97.106.161	China	147.237.76.201	e.atal.idf.il	drop	SAM rule	drop	1
191.96.249.18	Chile	147.237.76.34	yohalan.idf.il	drop		drop	1
180.97.106.162	China	147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	1
197.46.28.1	Egypt	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1
176.13.2.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
176.13.245.195	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.162	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1

08-17-2016-02:04:09 to 08-17-2016-03:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
96.246.225.112	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus/general/	Block	2
176.119.84.59	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
192.243.55.133	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
109.67.177.75	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
24.4.111.57	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
192.243.55.130	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=62215	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
217.132.232.3	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
124.171.205.81	Australia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19412-he/dover.aspx	Block	1
192.243.55.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
68.180.230.107	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
192.243.55.132	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/klali/default.asp?catid=59830&docid=70077	Block	1
79.180.135.69	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
172.56.2.31	United States	147.237.76.42	refuah.idf.il	Unauthorized Method POST for 147.237.76.42/894-he/refuah.aspx	Block	1
66.249.78.123	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
192.243.55.132	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1

08-17-2016-02:04:09 to 08-17-2016-03:04:09