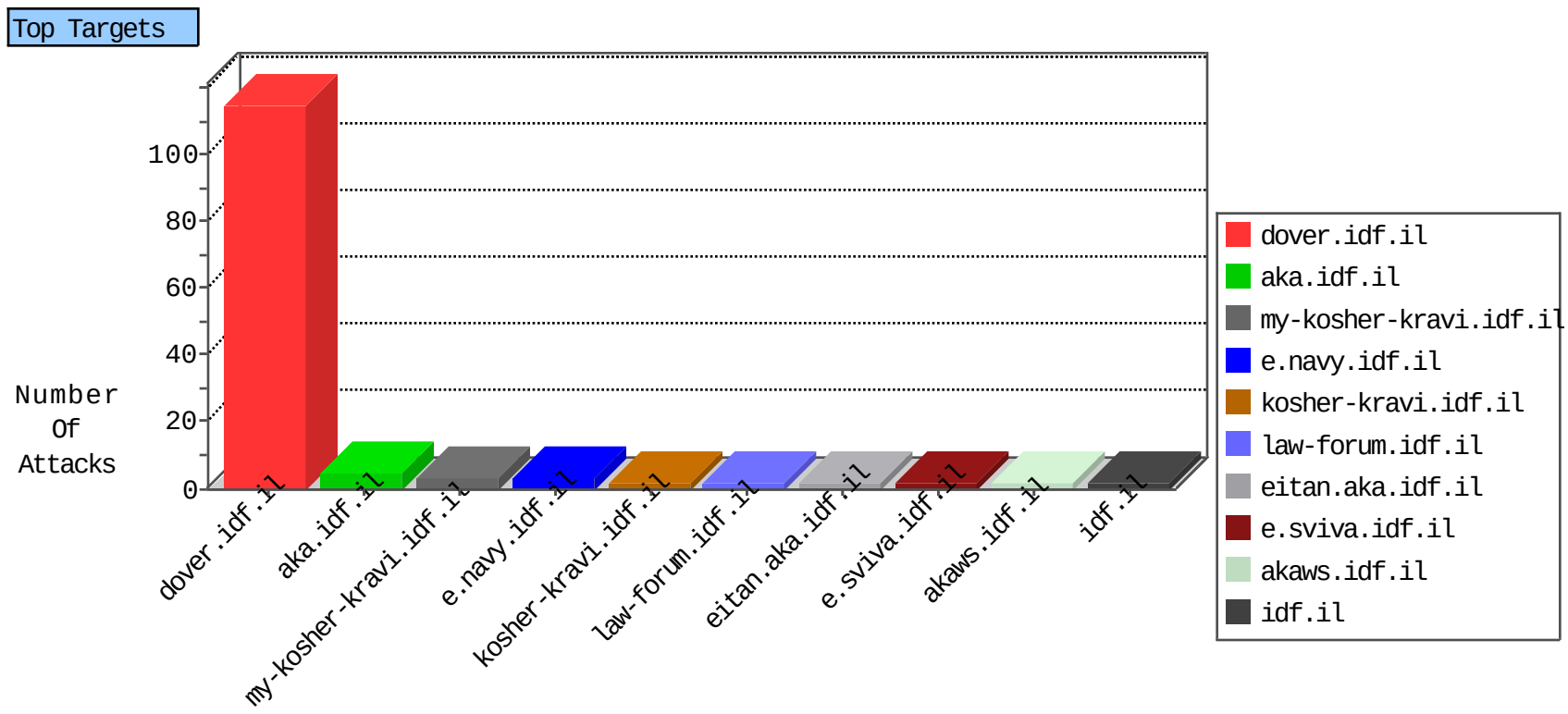
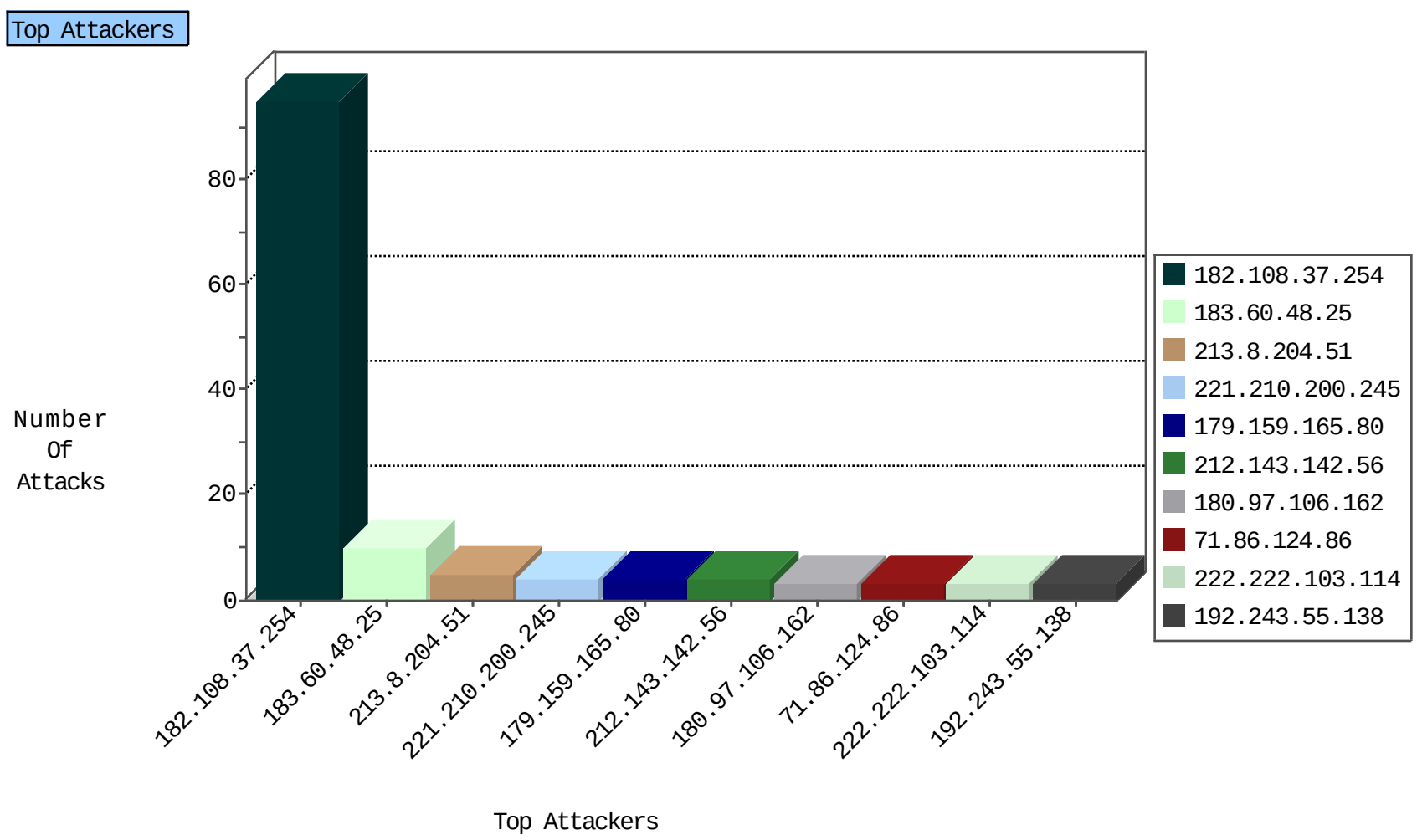
08-17-2016-01:08:22 to 08-17-2016-02:08:22

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-17-2016-01:08:22 to 08-17-2016-02:08:22

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
222.222.103.114	China	147.237.77.19	law-forum.idf.il	Invalid TCP Flags	drop	2
222.222.103.114	China	147.237.77.170	maarachot.idf.il	Invalid TCP Flags	drop	1
89.248.171.2	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1
185.158.112.59		147.237.76.196	e.sviva.idf.il	Black List	drop	1

08-17-2016-01:08:22 to 08-17-2016-02:08:22

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-17-2016-01:08:22 to 08-17-2016-02:08:22

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
182.108.37.254	147.237.77.216	China	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	2
71.86.124.86	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -f -sS	1
183.60.48.25	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
158.255.5.113	147.237.77.233	Russian Federation	atal.idf.il	ET SCAN NMAP -sS window 1024	1
221.210.200.245	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
113.108.10.31	147.237.77.243	China	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.210.200.245	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
71.86.124.86	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
183.60.48.25	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.0.33	China	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.210.200.245	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
158.255.5.113	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
221.210.200.245	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
71.86.124.86	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 4096	1
191.222.140.183	147.237.8.28	Brazil	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

08-17-2016-01:08:22 to 08-17-2016-02:08:22

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
179.159.165.80	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
186.227.38.122	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
180.97.106.162	China	147.237.0.16	my-kosher-kravi.idf.il	drop	SAM rule	drop	1
180.97.106.37	China	147.237.76.34	yohalan.idf.il	drop		drop	1
180.97.106.162	China	147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
66.249.64.134	Israel	147.237.0.33	idf.il	drop		drop	1
180.97.106.37	China	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
180.97.106.162	China	147.237.76.44	e.refuah.idf.il	drop	SAM rule	drop	1
176.13.12.145	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.161	China	147.237.0.35	akaws.idf.il	drop	SAM rule	drop	1
176.13.233.82	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
180.97.106.161	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1

08-17-2016-01:08:22 to 08-17-2016-02:08:22

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
182.108.37.254	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	46
182.108.37.254	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 182.108.37.254	Block	45
213.8.204.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	3
213.8.204.51	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	2
105.107.145.104	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
192.243.55.131	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	1
31.168.187.59	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
182.108.37.254	China	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/forms	Block	1
40.77.167.32	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
192.243.55.138	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	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
192.243.55.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58562&docid=35704	Block	1
68.180.230.172	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
182.108.37.254	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/11m.php	Block	1
192.243.55.138	United States	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	1

08-17-2016-01:08:22 to 08-17-2016-02:08:22