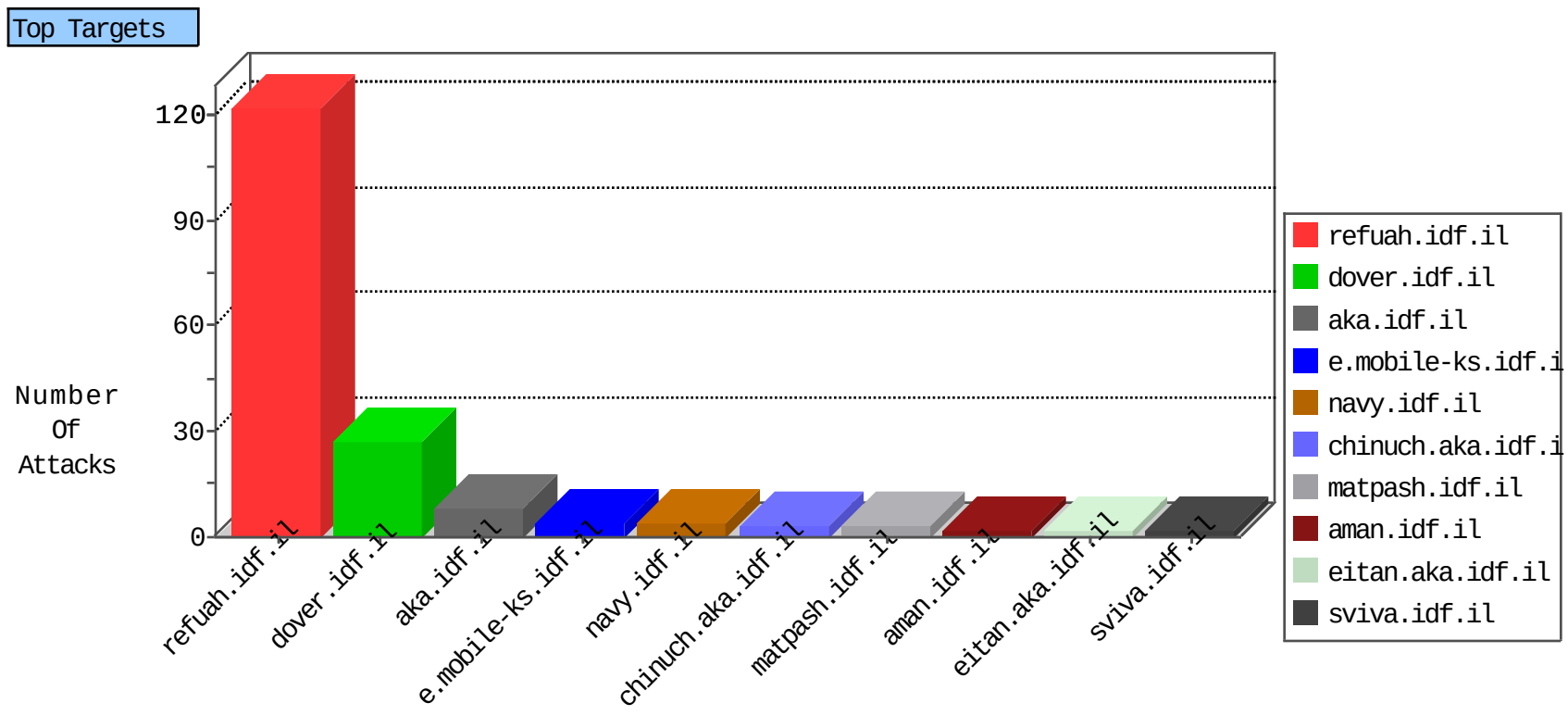
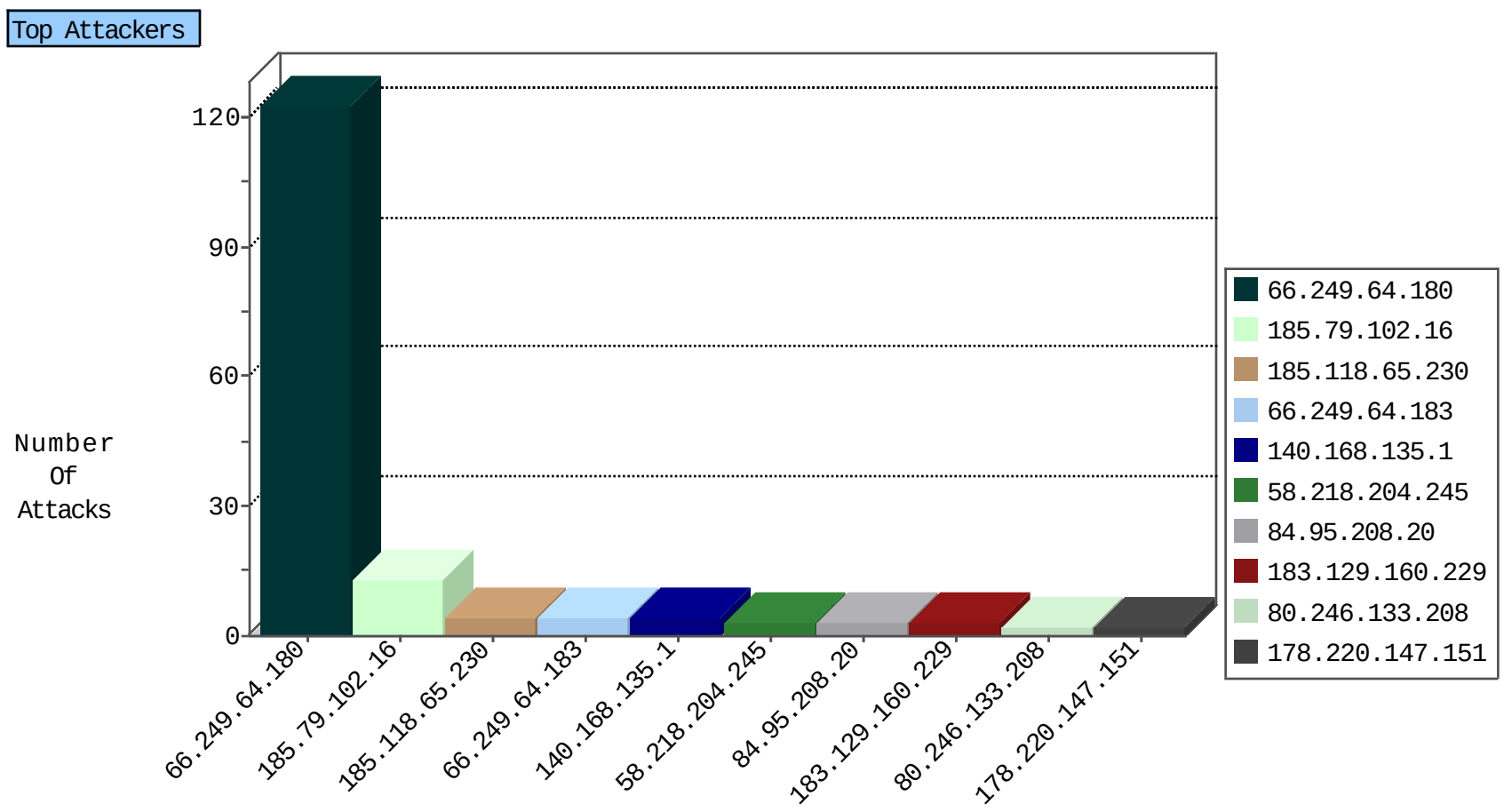
08-19-2016-07:04:05 to 08-19-2016-08:04:05

IDF Under Attack
Daily Report

Top Targets



Top Attackers



08-19-2016-07:04:05 to 08-19-2016-08:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.82.78.27	Netherlands	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
209.126.122.33	United States	147.237.76.30	himush.idf.il	Black List	drop	1

08-19-2016-07:04:05 to 08-19-2016-08:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.175	France	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.64	France	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
62.210.90.118	France	147.237.72.156	aman.idf.il	C1000074: HTTP: majestic bot	Permit	1

08-19-2016-07:04:05 to 08-19-2016-08:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.180	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	122
185.118.65.230	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	3
178.220.147.151	147.237.8.24		e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
163.172.169.150	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.73.185	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
59.100.214.202	147.237.76.200	Australia	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
58.218.204.245	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.118.65.230	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
181.62.254.202	147.237.76.39	Colombia	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
178.220.147.151	147.237.8.24		e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.85.139	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
122.179.41.212	147.237.77.226	India	www.chamatz.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.100.214.202	147.237.76.200	Australia	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
58.218.204.245	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
216.81.230.167	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1

08-19-2016-07:04:05 to 08-19-2016-08:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.79.102.16	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
183.129.160.229	China	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	2
122.167.233.213	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
140.168.135.1	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.77.227	e.hamaz.idf.il	drop	SAM rule	drop	1
140.168.135.1	Australia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1

08-19-2016-07:04:05 to 08-19-2016-08:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.183	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.183	Block	4
80.246.133.208	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
109.253.244.153	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
213.151.35.216	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	2
77.138.14.205	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/piwik.php	Block	1
66.249.79.170	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
66.249.64.180	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/08032011sufa.aspx	Block	1
66.249.79.173	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/yoman/enlarge.asp	Block	1
82.112.165.6	Lebanon	147.237.72.166	aka.idf.il	Unknown Parameter text1 in www.aka.idf.il/	None	1
207.46.13.9	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
68.58.133.202	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
62.210.90.118	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	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
66.249.69.245	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/general.aspx	Block	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	1
66.249.64.161	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/lomdim/forum/	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.79.170	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/edim/yoman/enlarge.asp	Block	1
66.249.64.174	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.tech.atal.idf.il/templates/sitemap/sitemap.aspx	Block	1

08-19-2016-07:04:05 to 08-19-2016-08:04:05