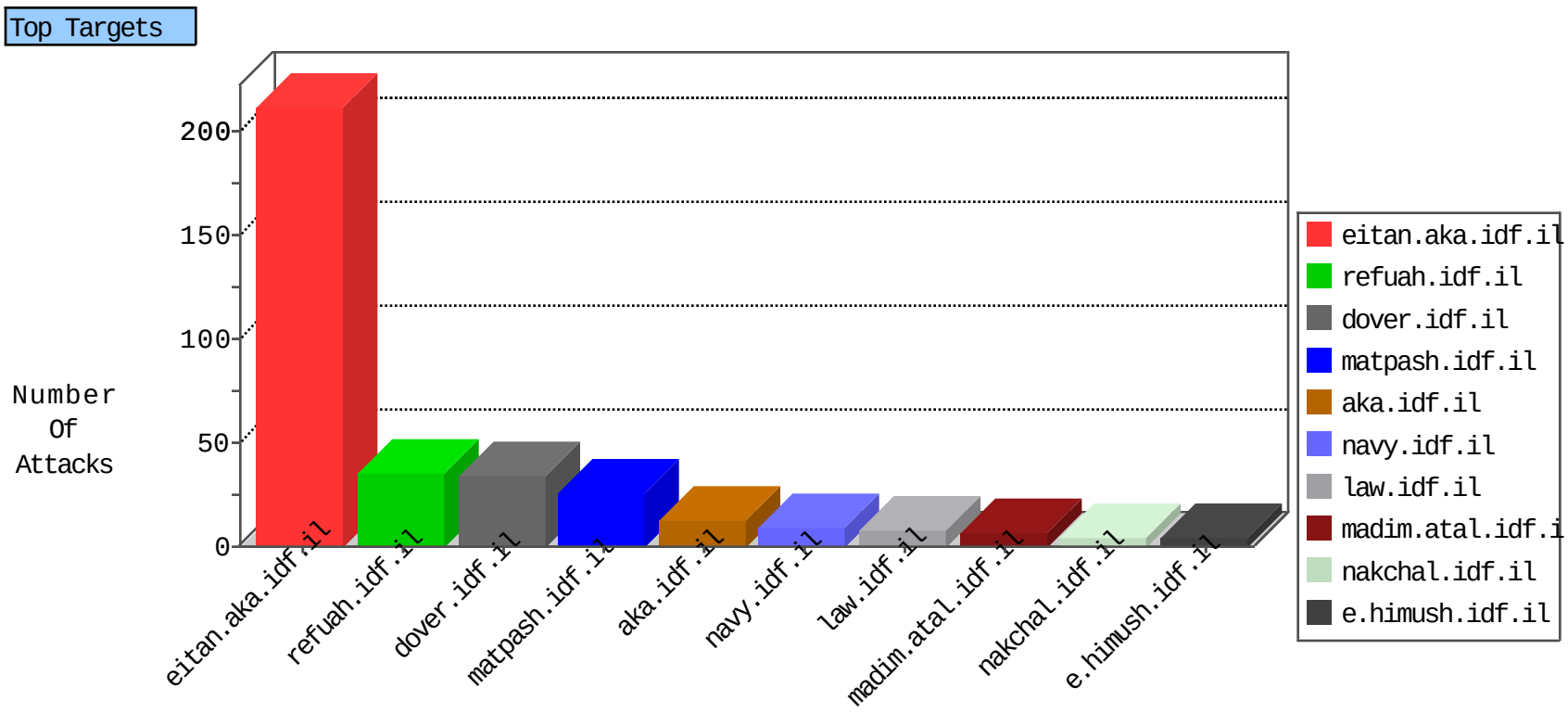
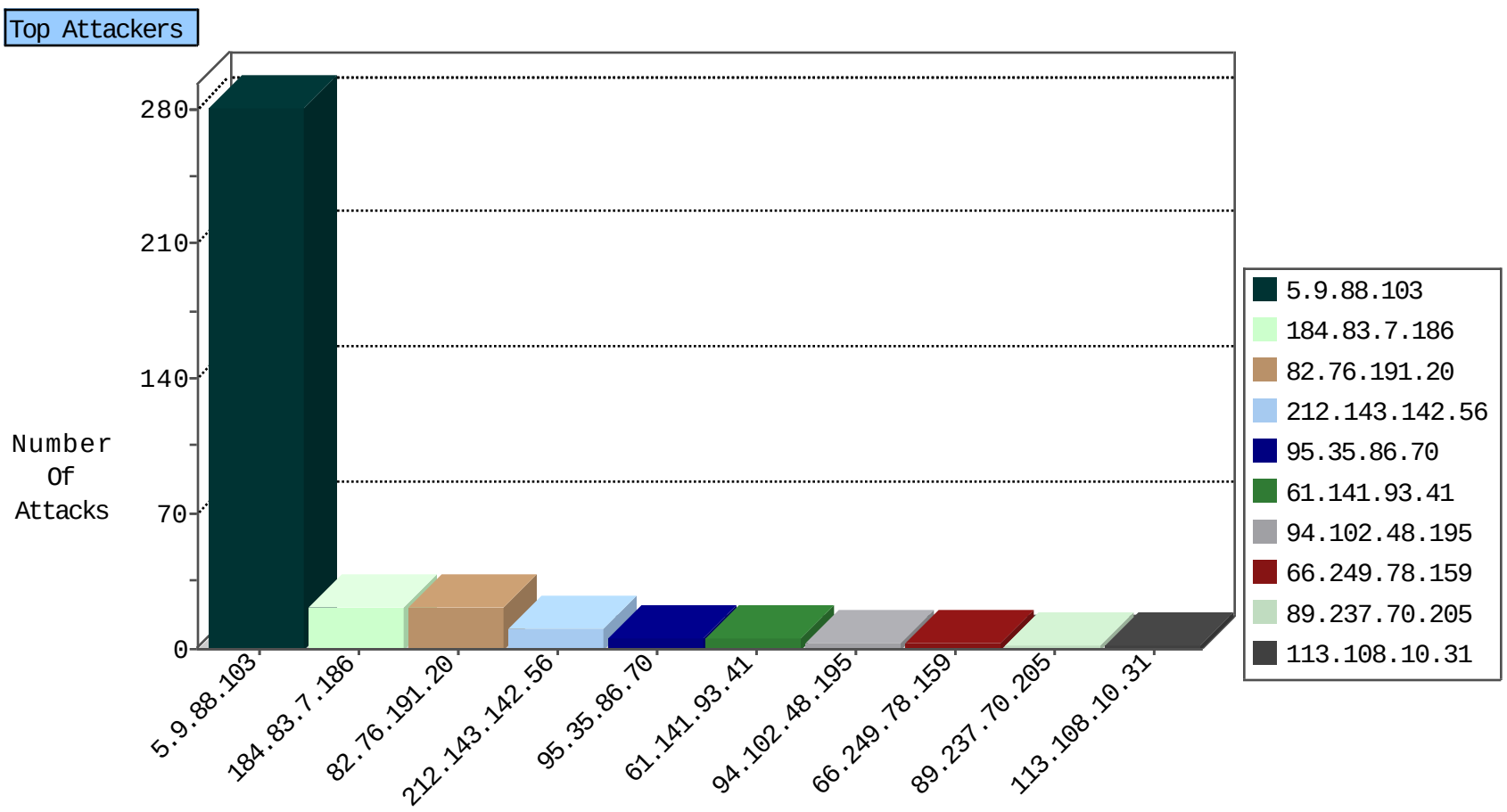
08-17-2016-06:04:05 to 08-17-2016-07:04:05

IDF Under Attack
Daily Report





08-17-2016-06:04:05 to 08-17-2016-07:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.158.200.93	Netherlands	147.237.76.197	e.himush.idf.il	Black List	drop	1
93.158.200.96	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
93.158.200.97	Netherlands	147.237.76.200	eitan.aka.idf.il	Black List	drop	1

08-17-2016-06:04:05 to 08-17-2016-07:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.88.103	Germany	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	210
5.9.88.103	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	32
5.9.88.103	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	19
5.9.88.103	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	7
5.9.88.103	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	6
5.9.88.103	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	3
5.9.88.103	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
5.9.88.103	Germany	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	2
182.50.130.133	Singapore	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	1

08-17-2016-06:04:05 to 08-17-2016-07:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
82.76.191.20	147.237.76.197	Romania	e.himush.idf.il	ET SCAN Potential SSH Scan	2
82.76.191.20	147.237.76.31	Romania	nakchal.idf.il	ET SCAN Potential SSH Scan	2
82.76.191.20	147.237.77.170	Romania	maarachot.idf.il	ET SCAN Potential SSH Scan	2
82.76.191.20	147.237.76.42	Romania	refuah.idf.il	ET SCAN Potential SSH Scan	2
82.76.191.20	147.237.77.121	Romania	e.navy.idf.il	ET SCAN Potential SSH Scan	2
113.108.10.31	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
82.76.191.20	147.237.76.38	Romania	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
82.76.191.20	147.237.77.235	Romania	sviva.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.156	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
82.76.191.20	147.237.77.216	Romania	dover.idf.il	ET SCAN Potential SSH Scan	1
82.76.191.20	147.237.77.61	Romania	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
185.29.11.182	147.237.76.86	Latvia	navy.idf.il	ET SCAN Potential SSH Scan	1
82.76.191.20	147.237.76.202	Romania	e.halag.idf.il	ET SCAN Potential SSH Scan	1
177.82.20.182	147.237.0.33	Brazil	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.76.191.20	147.237.76.199	Romania	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
113.108.10.31	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.148	Netherlands	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
82.76.191.20	147.237.76.34	Romania	yohalan.idf.il	ET SCAN Potential SSH Scan	1
93.158.215.182	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
82.76.191.20	147.237.76.30	Romania	himush.idf.il	ET SCAN Potential SSH Scan	1
82.76.191.20	147.237.77.227	Romania	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
54.153.99.128	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
82.76.191.20	147.237.77.176	Romania	matpash.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.77.205	United States	prisha.idf.il	ET DROP Dshield Block Listed Source	1
82.76.191.20	147.237.77.19	Romania	law-forum.idf.il	ET SCAN Potential SSH Scan	1
179.158.74.128	147.237.76.30	Brazil	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.76.191.20	147.237.76.200	Romania	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1

08-17-2016-06:04:05 to 08-17-2016-07:04:05

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	10
89.237.70.205	France	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
109.253.222.102	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
123.59.59.68	China	147.237.0.33	idf.il	drop		drop	1
216.218.206.71	United States	147.237.0.33	idf.il	drop		drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
184.83.7.186	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 184.83.7.186	Block	15
95.35.86.70	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	6
184.83.7.186	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	6
61.141.93.41	China	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 61.141.93.41	Block	4
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	2
61.141.93.41	China	147.237.77.74	law.idf.il	PHP Attempt	Block	1
109.65.170.93	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
61.141.93.41	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/499-en/contactus.php	Block	1
184.83.7.186	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.asp	Block	1
66.249.78.206	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/ 3שקופית	Block	1
144.76.236.183	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.76.52	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/.well-known/apple-app-site-association	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
157.55.39.237	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
84.229.41.152	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1