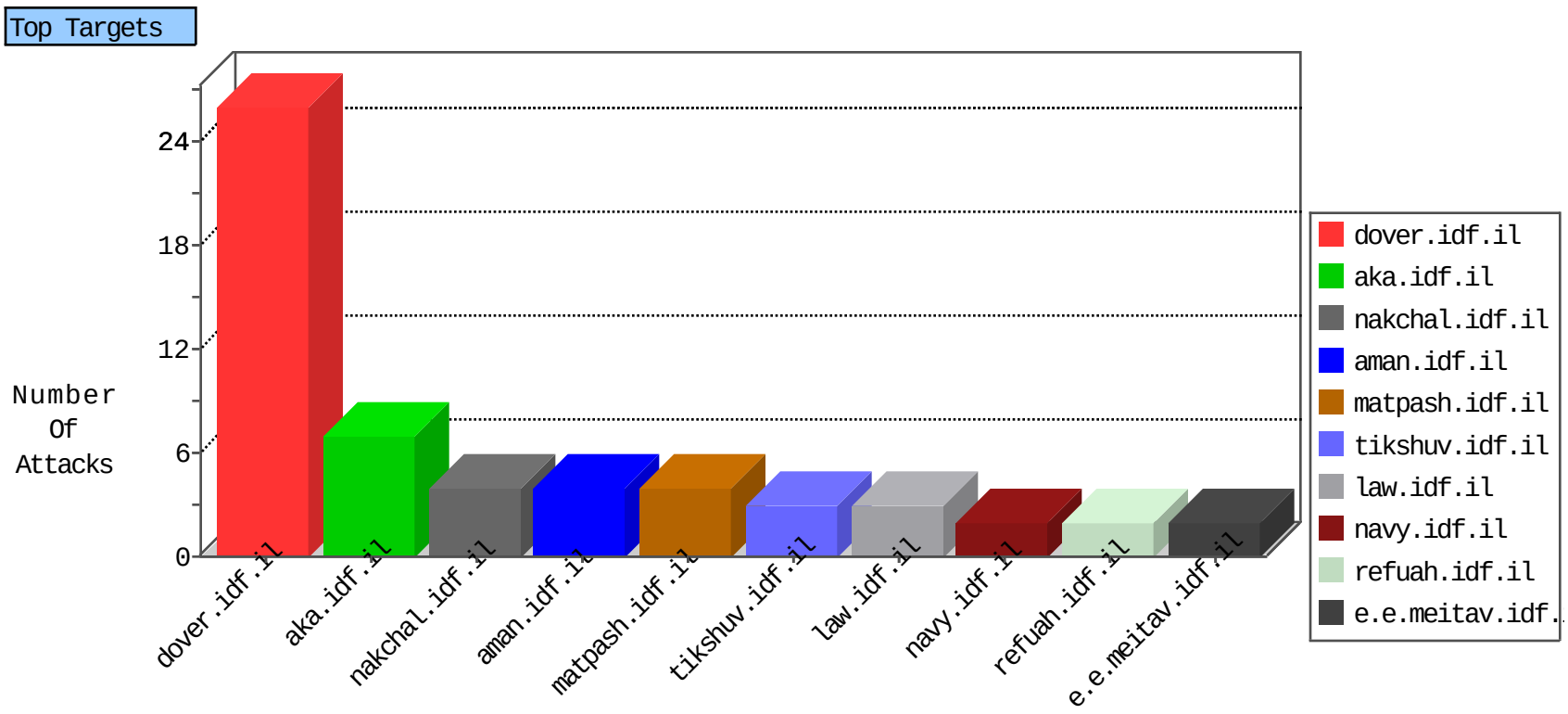
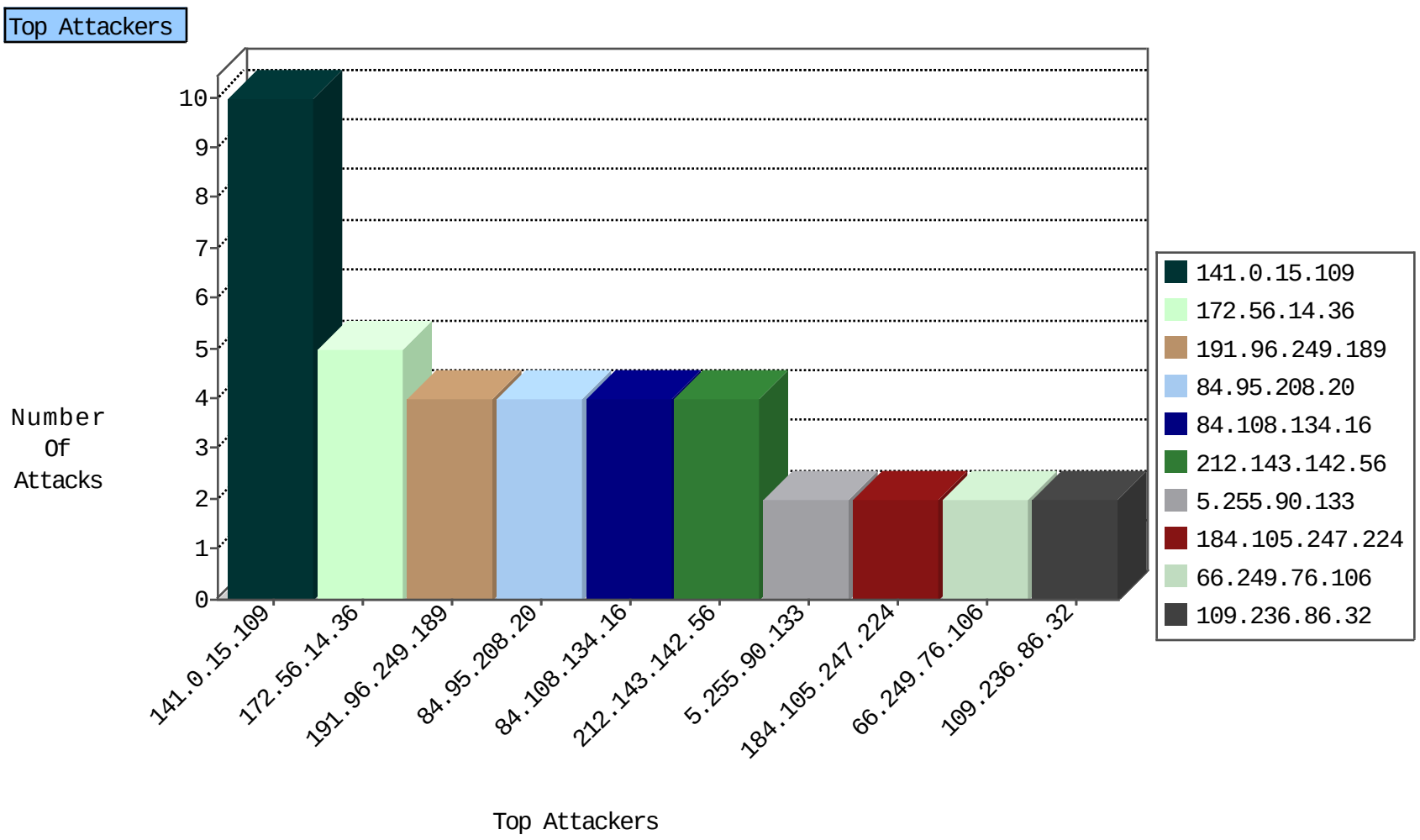
09-21-2016-05:04:03 to 09-21-2016-06:04:03

IDF Under Attack Daily Report





09-21-2016-05:04:03 to 09-21-2016-06:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.32.205.187	Netherlands	147.237.76.31	nakchal.idf.il	Black List	drop	1
192.69.91.141	United States	147.237.77.74	law.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
209.126.136.2	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
45.32.205.133	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1

09-21-2016-05:04:03 to 09-21-2016-06:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-21-2016-05:04:03 to 09-21-2016-06:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
191.96.249.189	147.237.77.74	Chile	law.idf.il	ET SCAN Potential SSH Scan	1
191.96.249.189	147.237.8.28	Chile	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
163.172.238.45	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
122.116.129.169	147.237.0.17	Taiwan	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.236.86.32	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.76.7	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
64.137.168.128	147.237.76.38	Canada	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
5.255.90.133	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.219.167	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
191.96.249.189	147.237.8.45	Chile	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
191.96.249.189	147.237.8.14	Chile	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
163.172.213.241	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
118.103.126.194	147.237.77.226	Japan	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.236.86.32	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.229.62.66	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
5.255.90.133	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

09-21-2016-05:04:03 to 09-21-2016-06:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
141.0.15.109	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
172.56.14.36	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
84.108.134.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
184.105.247.214	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.108.134.16	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
188.44.55.20	Russian Federation	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.174	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.224	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
189.128.13.225	Mexico	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.175	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.224	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.253.210.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.176.222.2	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
137.116.71.170	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.104	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.55	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
188.44.55.20	Russian Federation	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1

09-21-2016-05:04:03 to 09-21-2016-06:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter reffer in www.aka.idf.il/ishurim/main	None	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/briefing060102	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
66.249.64.108	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/masaiyot14092010.aspx	Block	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/general/piwik.php	Block	1
66.249.76.70	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
79.177.30.156	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1
66.249.64.112	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/speakerofmatpash/pages/tziudrefueitogaza13062011.aspx	Block	1
157.55.39.37	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.64.135	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/apple-app-site-association	Block	1
180.76.15.23	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/expand.js	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/iturim/asp/search.asp	None	1
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.65.22	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/1/1381.pdf	Block	1

09-21-2016-05:04:03 to 09-21-2016-06:04:03