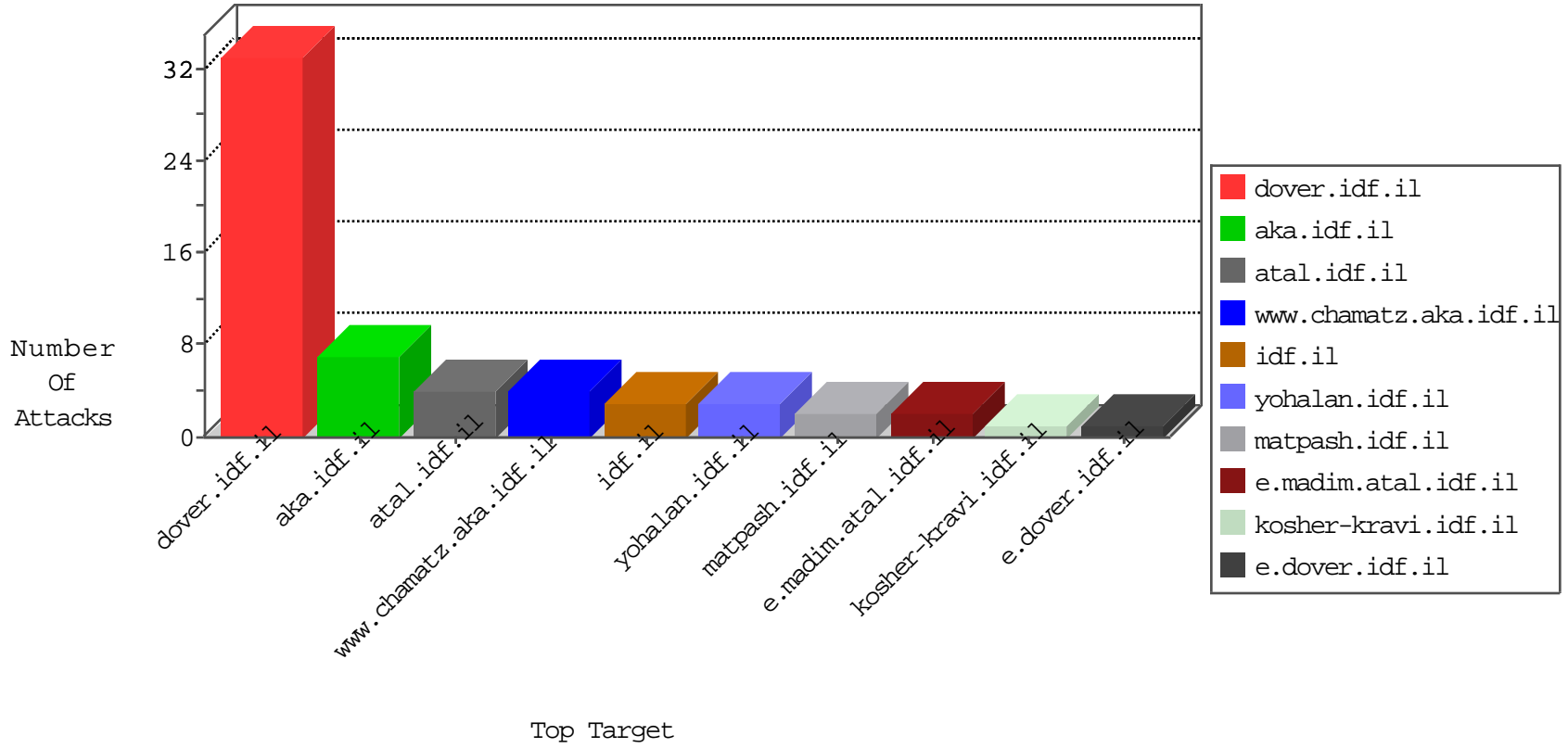


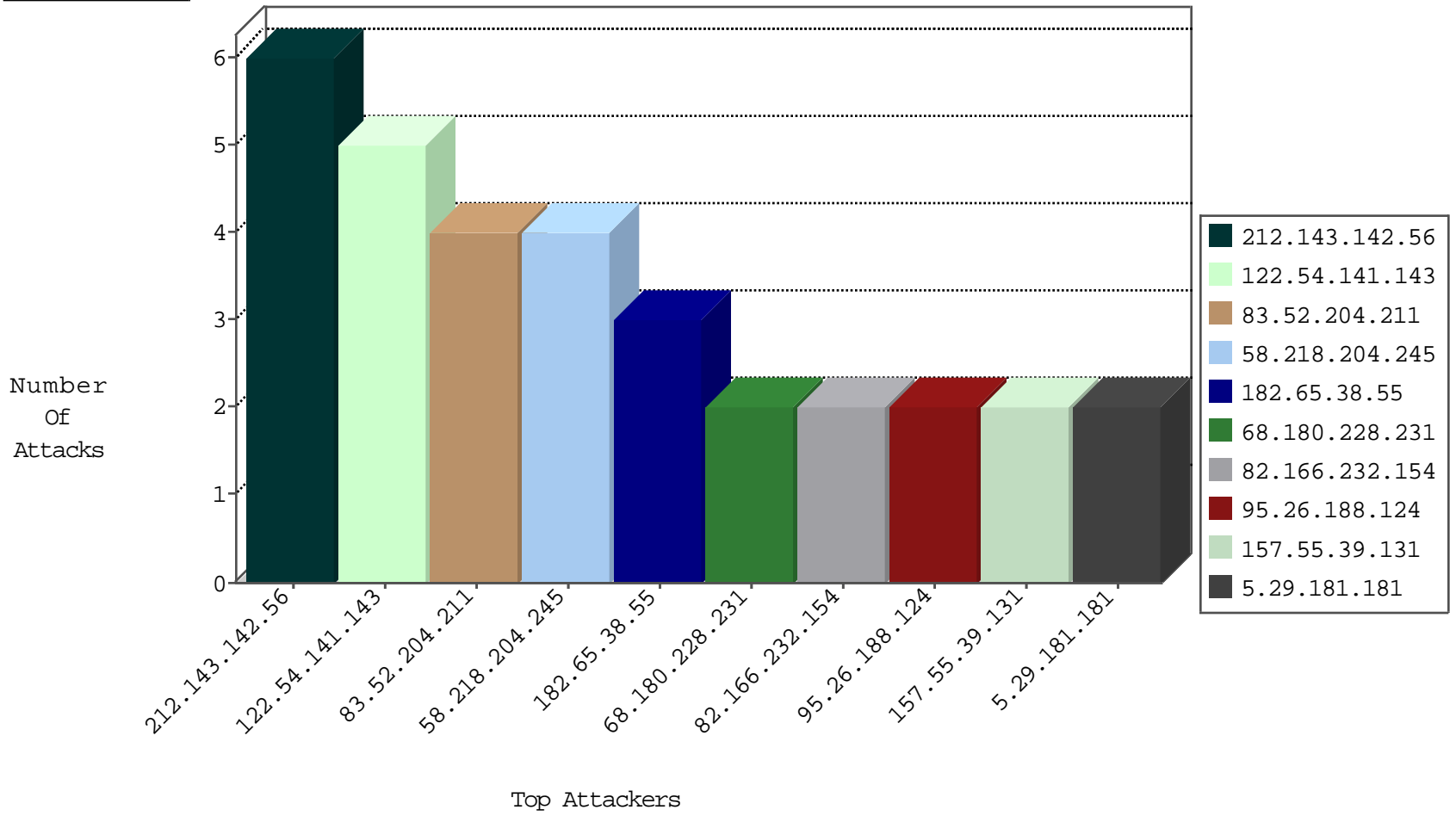
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

08-18-2016-03:04:08 to 08-18-2016-04:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
164.132.161.76	Italy	147.237.76.42	refuah.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.133.0	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	2
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
66.151.255.234	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.196	China	e.sviva.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
113.108.10.31	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
54.153.99.128	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
13.89.53.232	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.91.29	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.232.154	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
72.252.249.125	147.237.76.200	Jamaica	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.51	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
62.212.130.196	147.237.8.27	Netherlands	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
190.65.84.188	147.237.0.34	Colombia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.218.204.245	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
94.102.49.92	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
90.63.203.232	147.237.8.27	France	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

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	6
122.54.141.143	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
83.52.204.211	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
182.65.38.55	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
95.26.188.124	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	2
46.42.165.58	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.132	United States	147.237.0.33	idf.il	drop		drop	1
99.250.100.58	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.132	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
66.249.64.134	Israel	147.237.0.33	idf.il	drop		drop	1
109.253.222.106	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.133	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.131	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
157.55.39.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
5.29.165.67	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 141.8.132.78	Block	1
68.180.228.185	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/links/e.navy.idf.il/library/manage/resource/getfilecontent.hh.asp	Block	1
203.127.96.217	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.181.202.64	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
5.29.181.181	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1497-en/dover.aspx).	Block	1
68.180.228.185	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
82.166.232.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
5.29.181.181	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-he/cogat.aspx	Block	1
109.253.222.40	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.180.228.231	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1930-he/cogat.aspx	Block	1
136.243.16.208	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
77.139.201.104	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/forms.aspx	Block	1