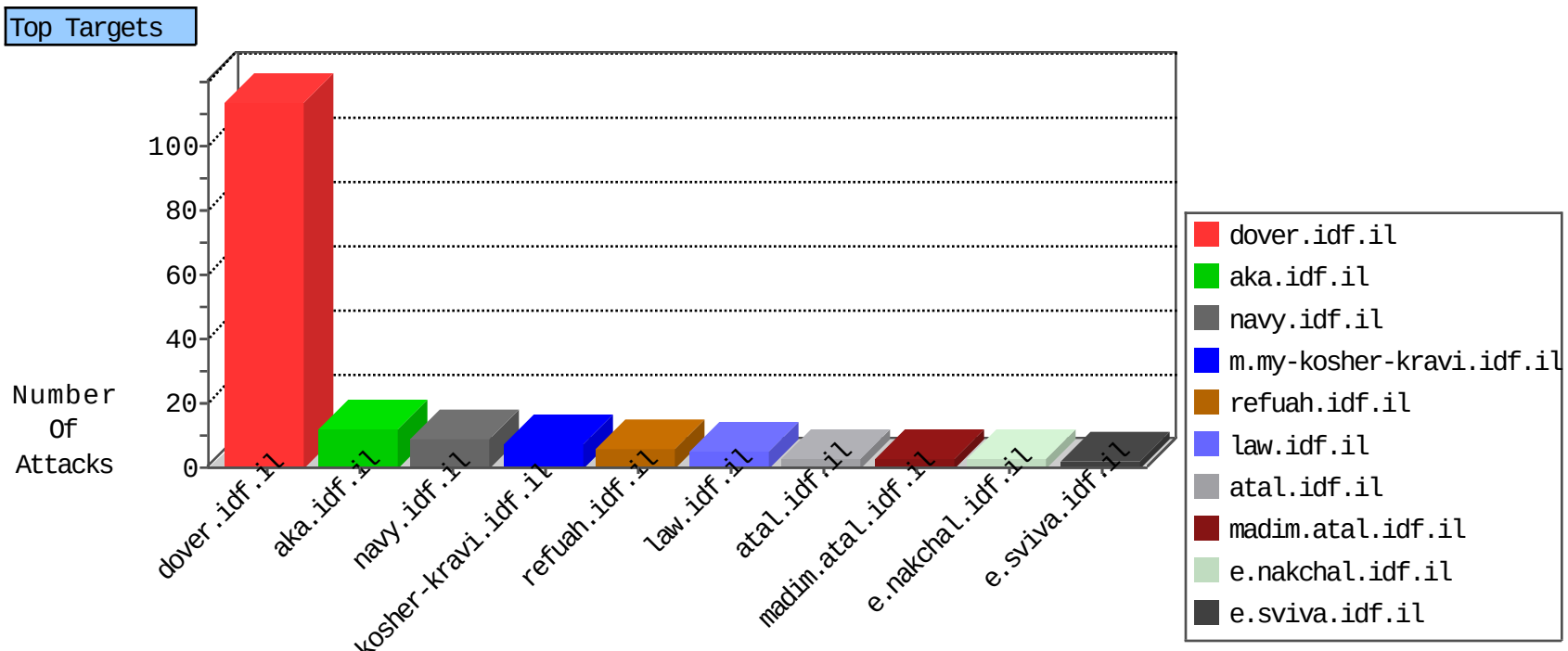
12-23-2015-05:04:07 to 12-23-2015-06:04:07

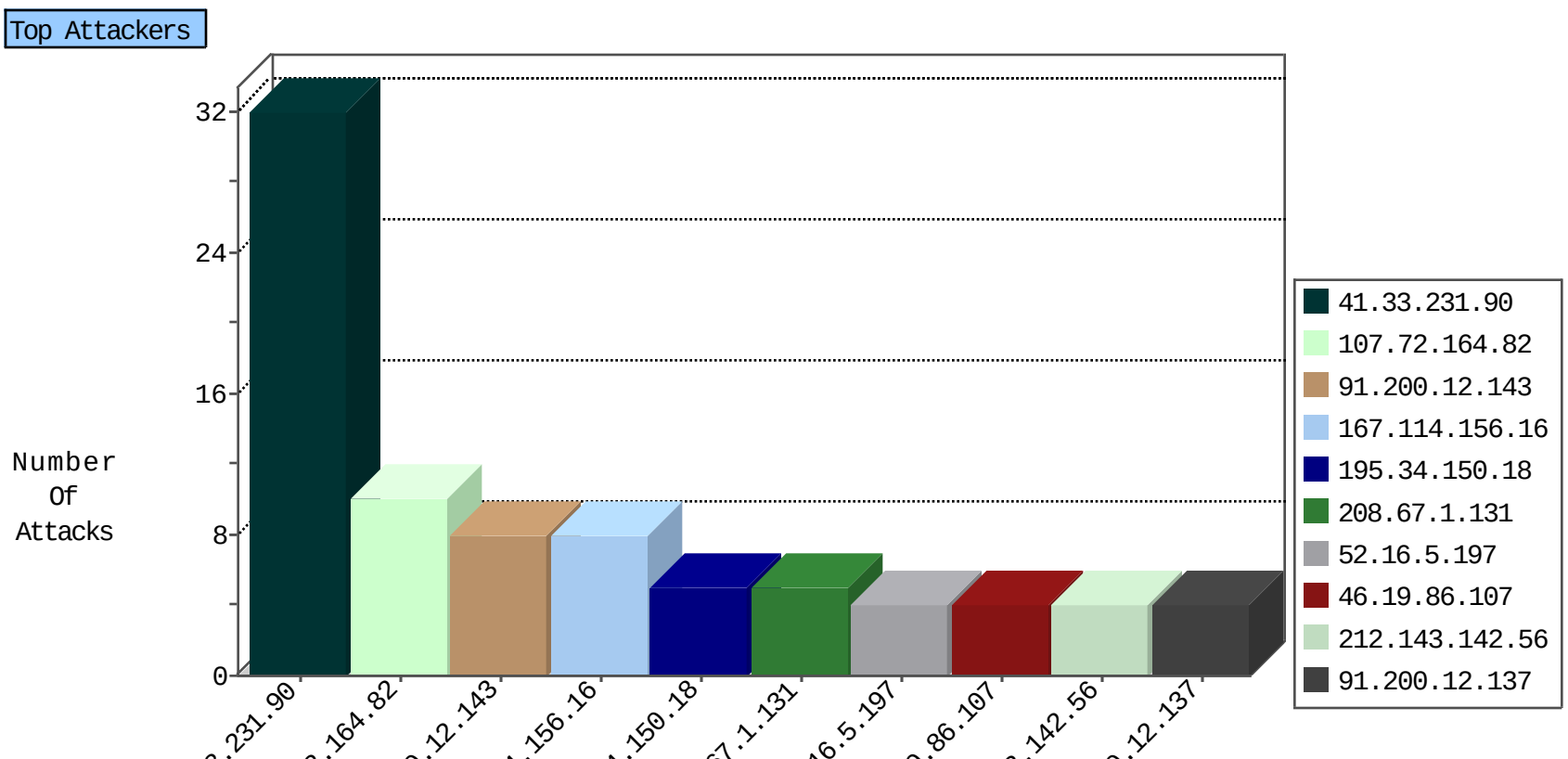
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

12-23-2015-05:04:07 to 12-23-2015-06:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	249
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
130.75.2.26	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	2
69.114.208.103	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
180.228.210.79	Korea, Republic of	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

12-23-2015-05:04:07 to 12-23-2015-06:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-23-2015-05:04:07 to 12-23-2015-06:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.75.201	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
66.249.79.75	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
131.109.15.15	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -f -sS	1
89.242.248.250	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.131	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
208.67.1.131	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.76.199	Cote D'Ivoire	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
196.47.173.21	147.237.76.199	Cote D'Ivoire	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
183.82.106.200	147.237.77.233	India	atal.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
131.109.15.15	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
116.77.177.69	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
208.67.1.131	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
208.67.1.131	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
23.96.213.135	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
208.67.1.131	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.76.199	Cote D'Ivoire	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
168.62.238.153	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
168.62.238.153	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

12-23-2015-05:04:07 to 12-23-2015-06:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
107.72.164.82	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
91.200.12.137	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
91.200.12.143	Ukraine	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
91.200.12.143	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
209.133.111.211	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
46.19.86.107	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence		monitor	2
46.19.86.107	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.80	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.87	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.58.245.111	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.107	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.112	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.88	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
31.168.1.226	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
46.117.245.187	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.122	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.170	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.116.25.197	Romania	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
46.117.245.187	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.122	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.171	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.229.192.88	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
137.175.19.122	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.46.13.184	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.184	Block	3
176.13.22.108	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
157.55.39.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/cmspages/getcss.aspx	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
77.125.163.231	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
195.154.194.111	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
62.219.226.71	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
24.135.66.196		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
157.55.39.55	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
77.125.163.231	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPersonalId in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	1
68.180.228.183	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
205.186.141.30	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
213.8.204.5	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
72.167.159.8	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/old/wp-admin/	Block	1
195.154.194.111	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
62.219.226.71	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 62.219.226.71	None	1
24.135.66.196		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
157.55.39.131	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.131	Block	1
78.128.92.193	Bulgaria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus×• ×'×—×¨×•	Block	1
183.206.168.44	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/system/fckeditor/editor/	Block	1
50.22.11.11	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/blog/wp-admin/	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
213.8.204.5	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
74.82.47.2	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
40.77.167.5	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/cmspages/getcss.aspx	Block	1
95.108.132.178	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2027-he/cogat.aspx	Block	1
207.46.13.184	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/api/visitorcountry/visitorcountry.svc/isvisitoreu	Block	1
184.105.139.70	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
54.154.209.228	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
117.20.3.74	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
77.125.6.61	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.79	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20786	Block	1
40.77.167.20	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 40.77.167.20	Block	1
173.54.44.94	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 173.54.44.94 (sigalgs DoS Attack)	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
70.32.68.20	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp/wp-admin/	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
188.138.1.218	Germany	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
54.154.209.228	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-includes/simplepie/theme-options.php	Block	1
2.54.153.56	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/tfasim.aspx.	Block	1
117.20.3.74	Australia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9692-he/refuah.aspx	Block	1
205.186.141.30	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1