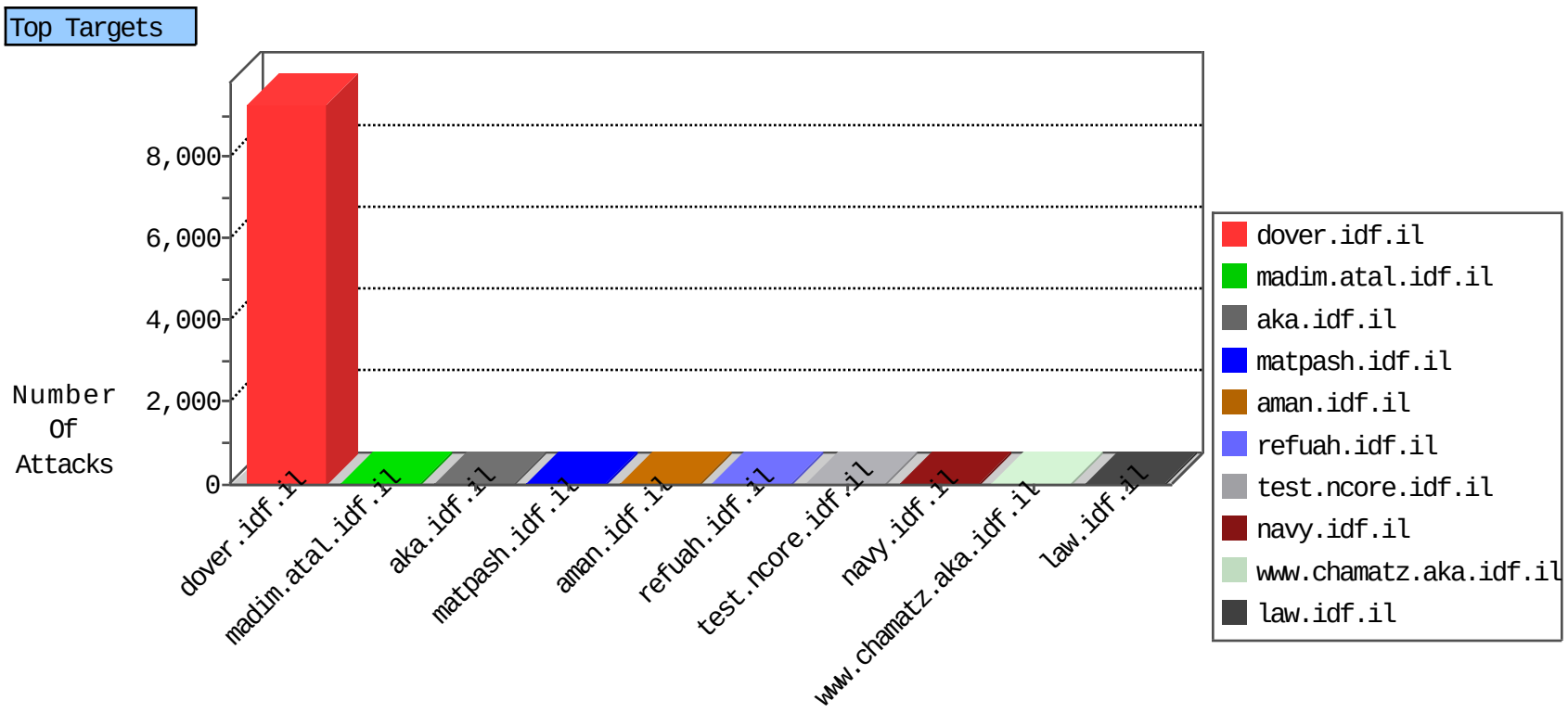
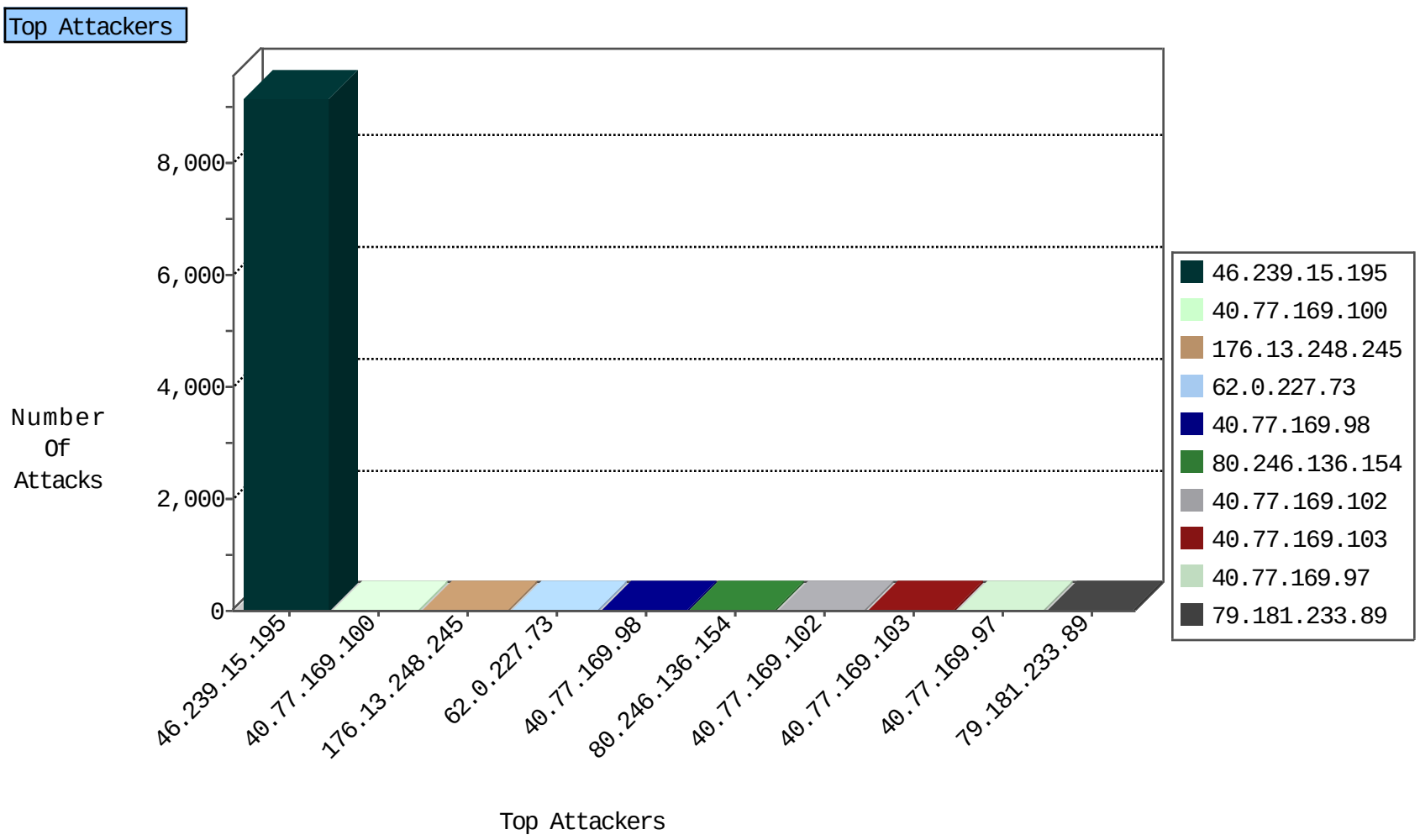
08-28-2016-07:04:01 to 08-28-2016-08:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-28-2016-07:04:01 to 08-28-2016-08:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.179	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
104.238.184.170	United Kingdom	147.237.76.86	navy.idf.il	Black List	drop	1
82.80.78.2	Israel	147.237.76.86	navy.idf.il	Black List	drop	1

08-28-2016-07:04:01 to 08-28-2016-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.212.73.211	Netherlands	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
192.166.218.214	Poland	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	2
192.166.218.214	Poland	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

08-28-2016-07:04:01 to 08-28-2016-08:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.165.253.25	147.237.77.235	Germany	sviva.idf.il	ET SCAN Potential SSH Scan	1
208.73.143.36	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
183.129.160.229	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
163.172.220.43	147.237.0.34	United Kingdom	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
143.0.115.31	147.237.76.177	Brazil	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
103.207.36.164	147.237.76.176	Vietnam	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
72.252.24.133	147.237.76.176	Jamaica	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
72.252.24.133	147.237.76.176	Jamaica	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
46.227.67.172	147.237.8.28	Sweden	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
201.38.68.132	147.237.76.176	Brazil	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.220.43	147.237.76.31	United Kingdom	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.76.176	United Kingdom	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
143.0.115.31	147.237.76.177	Brazil	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
72.252.24.133	147.237.76.176	Jamaica	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
66.249.76.117	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

08-28-2016-07:04:01 to 08-28-2016-08:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8044
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	200
62.0.227.73	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
40.77.169.100	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	7
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
40.77.169.100	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	7
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
40.77.169.98	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
79.181.233.89	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
188.32.128.58	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
194.165.146.148	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.104	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
40.77.169.103	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
159.203.33.10	Canada	147.237.0.200	m4u.idf.il	drop		drop	1
188.255.99.141	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.156.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.225.88	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
109.253.198.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.236.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
66.249.90.51	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
118.173.177.206	Thailand	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
216.218.206.120	United States	147.237.0.33	idf.il	drop		drop	1
139.162.179.166	United States	147.237.0.35	akaws.idf.il	drop		drop	1

08-28-2016-07:04:01 to 08-28-2016-08:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.248.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
80.246.136.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
182.74.65.110	India	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
40.77.169.96	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/m/main/giyus/general.aspx	Block	2
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
94.188.161.26	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 94.188.161.26	Block	2
2.53.176.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
94.188.161.26	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/6/size338x0/1806.jpg	Block	2
85.65.79.82	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.65.79.82	Block	2
40.77.169.99	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.130.109	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/size100x0/2294.jpg	Block	1
212.129.62.79	France	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on 147.237.77.170/	Block	1
157.55.39.252	United States	147.237.72.166	aka.idf.il	Unknown Parameter pagenum in aka.idf.il/chinuch/gallery/	None	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/enlarge.asp	Block	1
46.19.86.109	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.119	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
66.249.64.107	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/9/1209.pdftextgreater	Block	1
212.179.104.26	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
176.13.16.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.127	Israel	147.237.77.226	www.chamatz.aka.idf.il	Abnormally Long Request method	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/giyus/general.aspx	Block	1
46.121.63.50	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.121.63.50	Block	1
195.154.41.132	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
31.154.81.71	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
157.55.39.144	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/www.tikshuv.idf.il	Block	1
82.81.40.211	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mail	Block	1
66.249.64.115	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector/	Block	1
212.179.104.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
176.13.17.253	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
46.19.85.127	Israel	147.237.77.226	www.chamatz.aka.idf.il	Malformed URL	Block	1
109.66.33.165	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/sachar/undefined	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.121.220.166	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.111	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-19142-en/dover.aspx i	Block	1
157.55.39.173	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_text.asp	Block	1
66.249.64.116	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/nakba15052011.aspx	Block	1
46.19.85.127	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unknown HTTP Request Method he-IL,he;q=0.8,en-US;q=0.6,en;q=0.4 in URL	Block	1
141.226.162.241	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
68.180.230.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
212.76.102.249	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
157.55.39.252	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/kamlar/gallery/	None	1
85.65.79.82	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
180.151.15.250	India	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/miluim/templates/inner.asp	Block	1

08-28-2016-07:04:01 to 08-28-2016-08:04:01