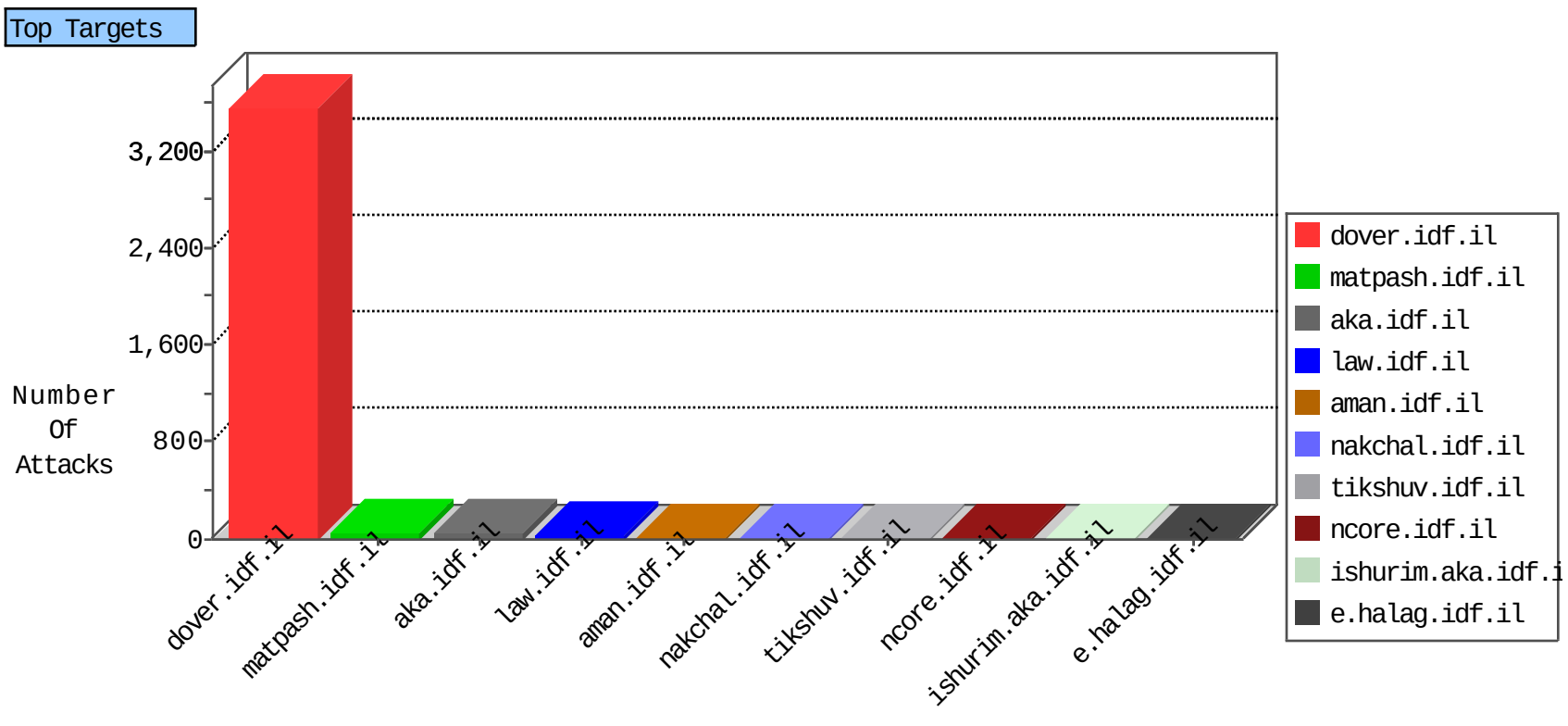
08-28-2016-05:04:09 to 08-28-2016-06:04:09

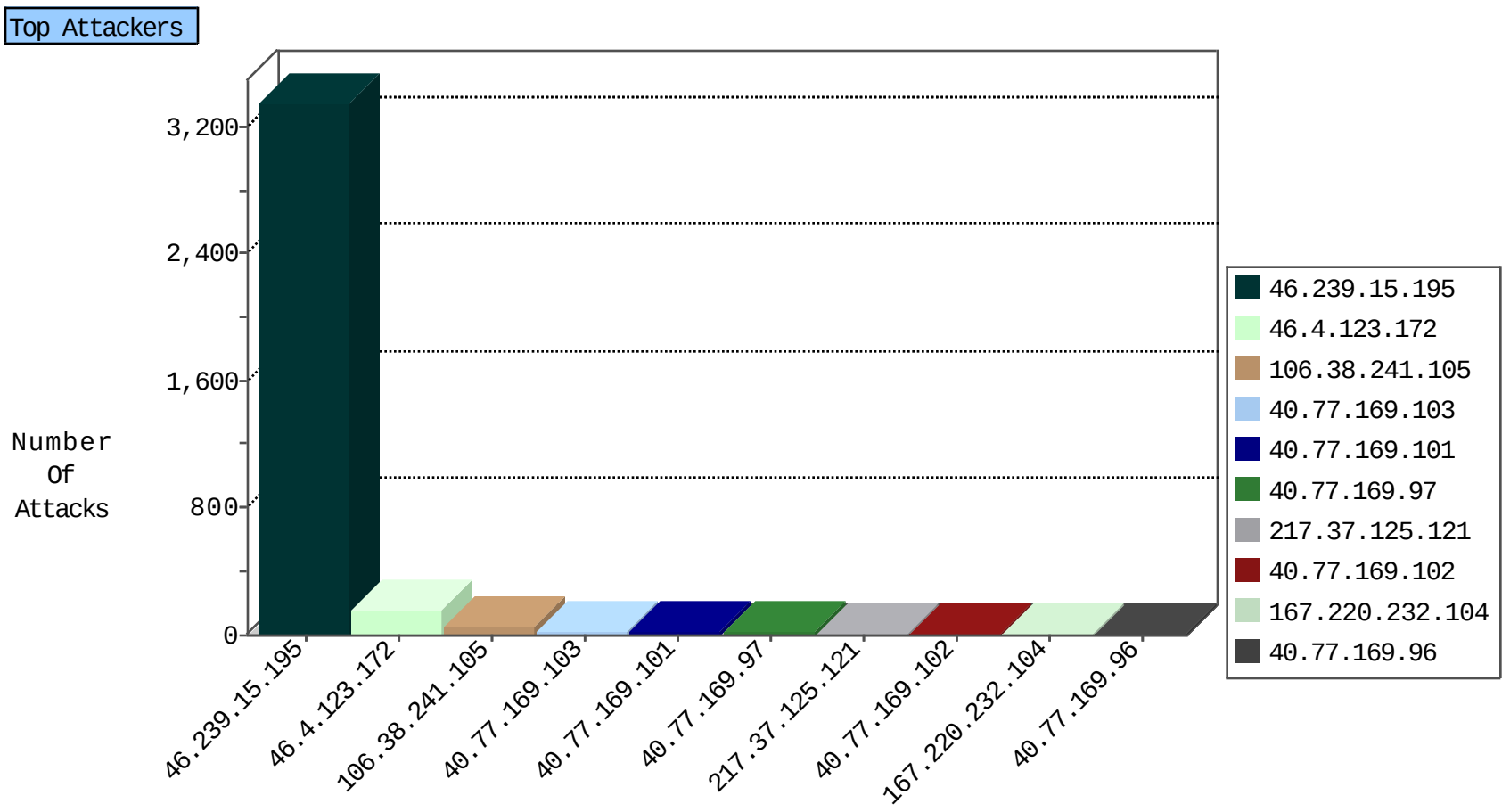
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-28-2016-05:04:09 to 08-28-2016-06:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.76.177	ncore.idf.il	Black List	drop	2
104.238.184.170	United Kingdom	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

08-28-2016-05:04:09 to 08-28-2016-06:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.123.172	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	98
46.4.123.172	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	36
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	21
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	17
46.4.123.172	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	10
46.4.123.172	Germany	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	8
217.37.125.121	United Kingdom	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
46.4.123.172	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	5
106.38.241.105	China	147.237.72.156	aman.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
106.38.241.105	China	147.237.76.86	navy.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
106.38.241.105	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

08-28-2016-05:04:09 to 08-28-2016-06:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
217.37.125.121	147.237.77.74	United Kingdom	law.idf.il	SQL Injection - Select From	8
183.129.160.229	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
159.203.33.10	147.237.76.177	Canada	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
45.55.8.238	147.237.0.200	United States	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
13.78.113.110	147.237.76.202	Japan	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
188.0.236.165	147.237.72.167	Moldova, Republic of	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
163.172.220.43	147.237.76.196	United Kingdom	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
128.199.81.128	147.237.72.166	Singapore	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
71.6.165.200	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
13.78.113.110	147.237.77.61	Japan	e.cogat.idf.il	ET SCAN NMAP -sS window 3072	1
13.78.113.110	147.237.76.202	Japan	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1

08-28-2016-05:04:09 to 08-28-2016-06:04:09

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	3101
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	250
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
40.77.169.101	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	13
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
167.220.232.104	Japan	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
40.77.169.101	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
40.77.169.96	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
40.77.169.97	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	5
40.77.169.103	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
41.102.31.178	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
201.255.46.38	Argentina	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	2
40.77.169.104	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
40.77.169.97	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
183.129.160.229	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
176.13.244.211	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
176.58.124.35	United Kingdom	147.237.0.200	m4u.idf.il	drop		drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
183.129.160.229	China	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
159.203.33.10	Canada	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
183.129.160.229	China	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1

08-28-2016-05:04:09 to 08-28-2016-06:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
74.64.19.138	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	2
65.55.213.31	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
40.77.169.96	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
212.71.254.175	United Kingdom	147.237.0.34	tikshuv.idf.il	Unauthorized HTTP Method	Block	1
79.183.6.27	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	1
178.255.87.242	United Kingdom	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/robots.txt	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.169.96	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
212.71.254.175	United Kingdom	147.237.0.34	tikshuv.idf.il	Unauthorized Method OPTIONS for /	Block	1
84.108.238.47	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
199.30.24.108	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jenin.stm" target="_blank	Block	1
213.8.204.66	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
131.253.25.147	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	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
207.46.13.64	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/announcements/2002/june/mazen.stm</dd><dd>	Block	1
74.64.19.138	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 74.64.19.138	Block	1
46.121.63.50	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/3468.gif	Block	1
157.55.39.93	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/library/generaldoc.asp	Block	1
207.46.13.110	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
157.55.39.175	United States	147.237.72.166	aka.idf.il	Unknown Parameter pagenum in aka.idf.il/chinuch/gallery/	None	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1

08-28-2016-05:04:09 to 08-28-2016-06:04:09