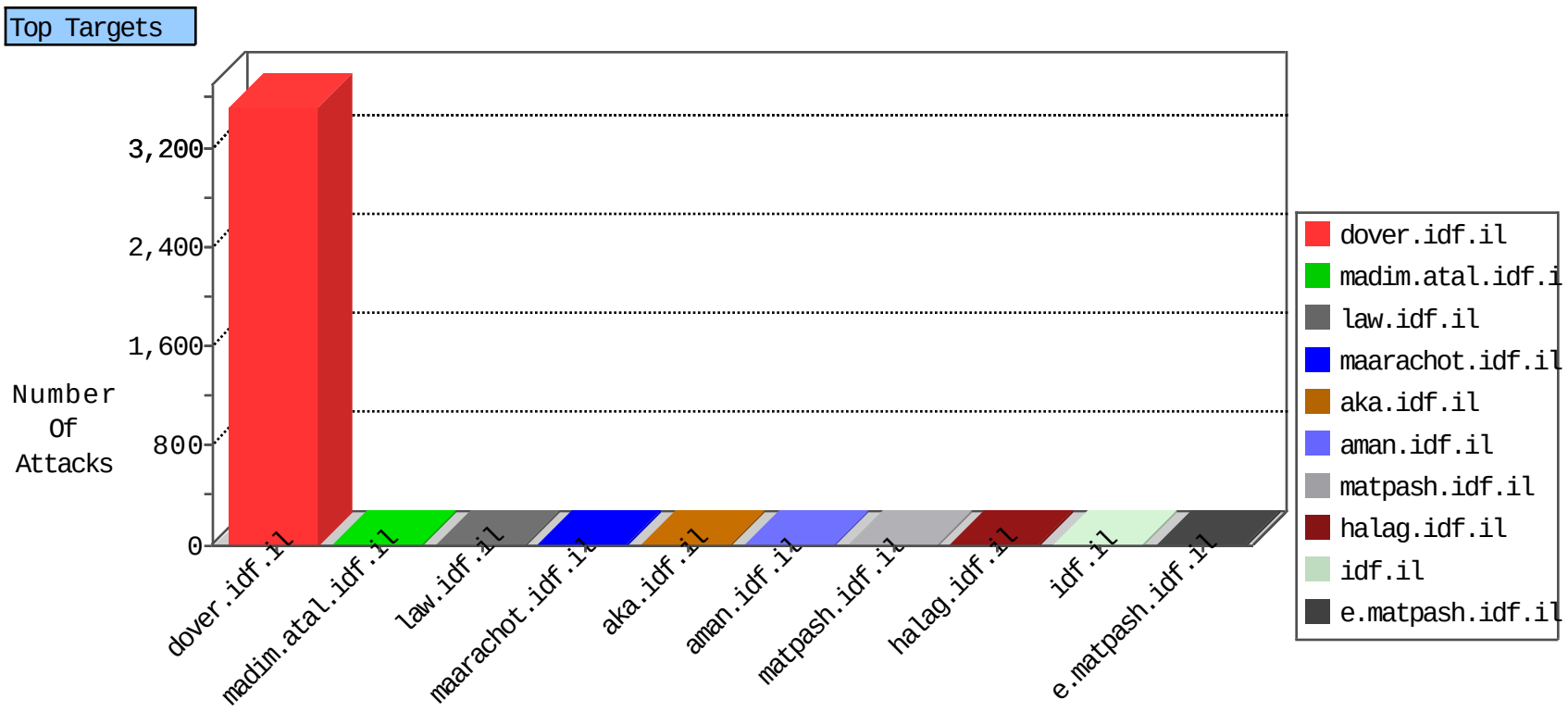
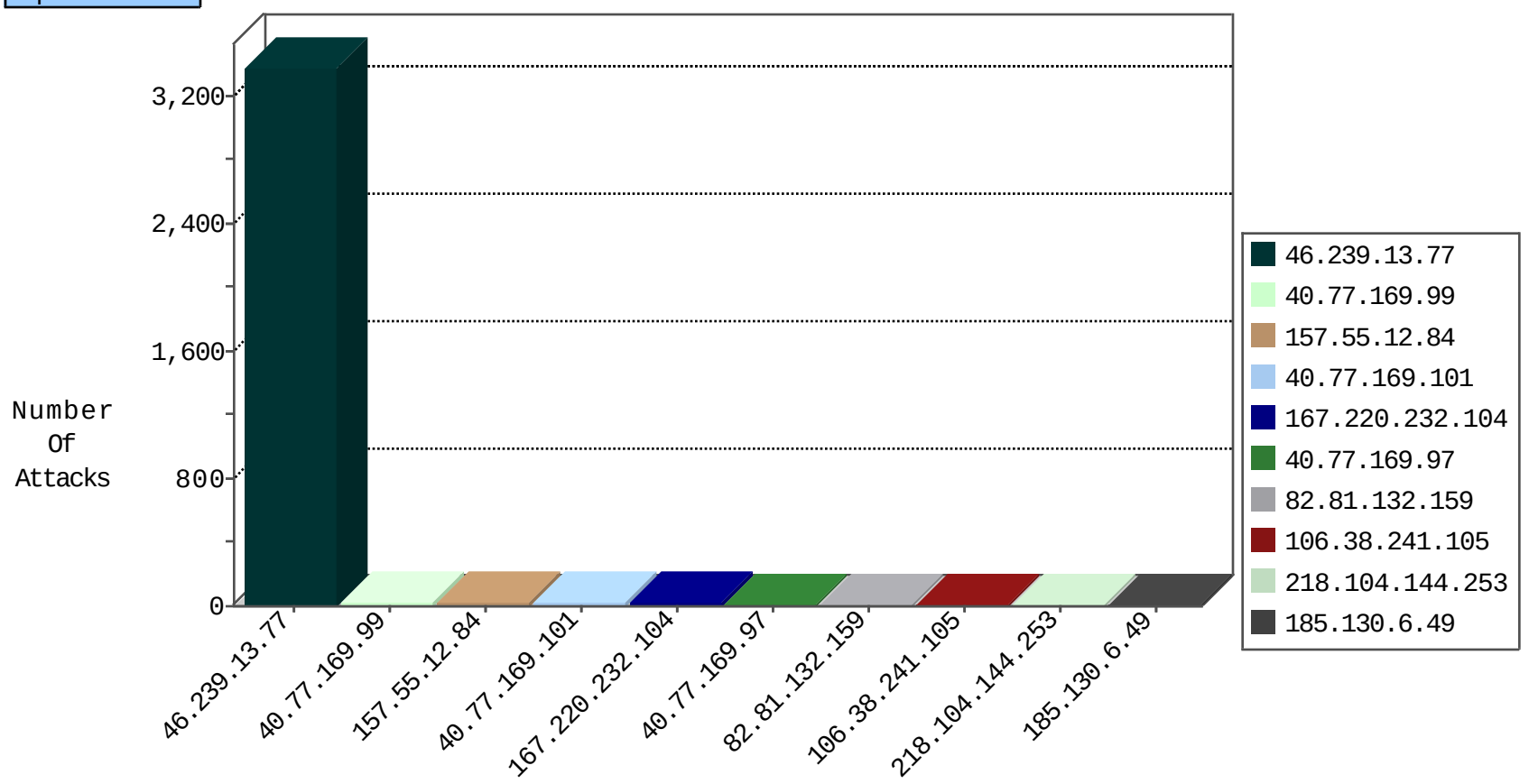
08-27-2016-09:04:03 to 08-27-2016-10:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-27-2016-09:04:03 to 08-27-2016-10:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	4

08-27-2016-09:04:03 to 08-27-2016-10:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.6.49	Lithuania	147.237.77.170	maarachot.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
185.130.6.49	Lithuania	147.237.77.170	maarachot.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
198.20.69.74	United States	147.237.76.44	e.refuah.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

08-27-2016-09:04:03 to 08-27-2016-10:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
176.13.20.232	147.237.77.176	Israel	matpash.idf.il	ET SCAN NMAP -sA (2)	1
218.104.144.253	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
137.117.168.203	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
218.104.144.253	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
123.206.73.185	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
218.104.144.253	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
66.203.215.242	147.237.77.227	Canada	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
201.38.68.132	147.237.77.121	Brazil	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
193.36.35.241	147.237.77.178	Russian Federation	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
188.0.236.165	147.237.77.205	Moldova, Republic of	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
188.0.236.165	147.237.77.178	Moldova, Republic of	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
185.130.6.49	147.237.77.170	Lithuania	maarachot.idf.il	ET WEB_SERVER Muieblackcat scanner	1
218.104.144.253	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
163.172.169.150	147.237.77.243	United Kingdom	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.104.144.253	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
123.206.73.185	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
218.104.144.253	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
66.249.65.152	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	1
218.104.144.253	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
198.52.97.88	147.237.77.74	United States	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
188.0.236.165	147.237.77.205	Moldova, Republic of	prisha.idf.il	ET SCAN Potential SSH Scan	1
188.0.236.165	147.237.77.179	Moldova, Republic of	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
188.0.236.165	147.237.77.178	Moldova, Republic of	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1

08-27-2016-09:04:03 to 08-27-2016-10:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.13.77	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3232
46.239.13.77	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	150
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
167.220.232.104	Japan	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
167.220.232.104	Japan	147.237.77.74	law.idf.il	drop	SAM rule	drop	8
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
176.13.19.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
40.77.169.101	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	4
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
193.111.140.153	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.181.21.41	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
176.67.98.161	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
106.38.241.105	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	2
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
74.82.47.18	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
106.38.241.105	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
109.253.209.227	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
46.19.86.222	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
2.87.114.97	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.121.182	United States	147.237.0.33	idf.il	drop		drop	1
104.158.35.213	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
183.129.160.229	China	147.237.0.200	m4u.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
31.168.172.147	Israel	147.237.0.35	akaws.idf.il	drop		drop	1
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
184.105.247.200	United States	147.237.0.33	idf.il	drop		drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
37.247.36.105	Netherlands	147.237.0.35	akaws.idf.il	drop		drop	1

08-27-2016-09:04:03 to 08-27-2016-10:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
157.55.12.84	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	24
82.81.132.159	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
40.77.169.100	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
65.55.210.136	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.160.29	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
40.77.169.98	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
131.253.27.20	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
40.77.169.102	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.186.90.255	Israel	147.237.72.156	aman.idf.il	Malformed URL www.aman.idf.il:443	Block	1
66.249.75.8	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
199.30.24.123	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.139.46.255	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
109.186.90.255	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 109.186.90.255 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
219.75.81.93	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.179.51.60	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.64.59	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/trajector/	Block	1
109.186.90.255	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.112	Block	1
220.255.145.120	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.177	Block	1
68.180.230.171	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
109.64.166.79	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/login.aspx	None	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/generic/	Block	1
77.138.147.12	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	1

08-27-2016-09:04:03 to 08-27-2016-10:04:03