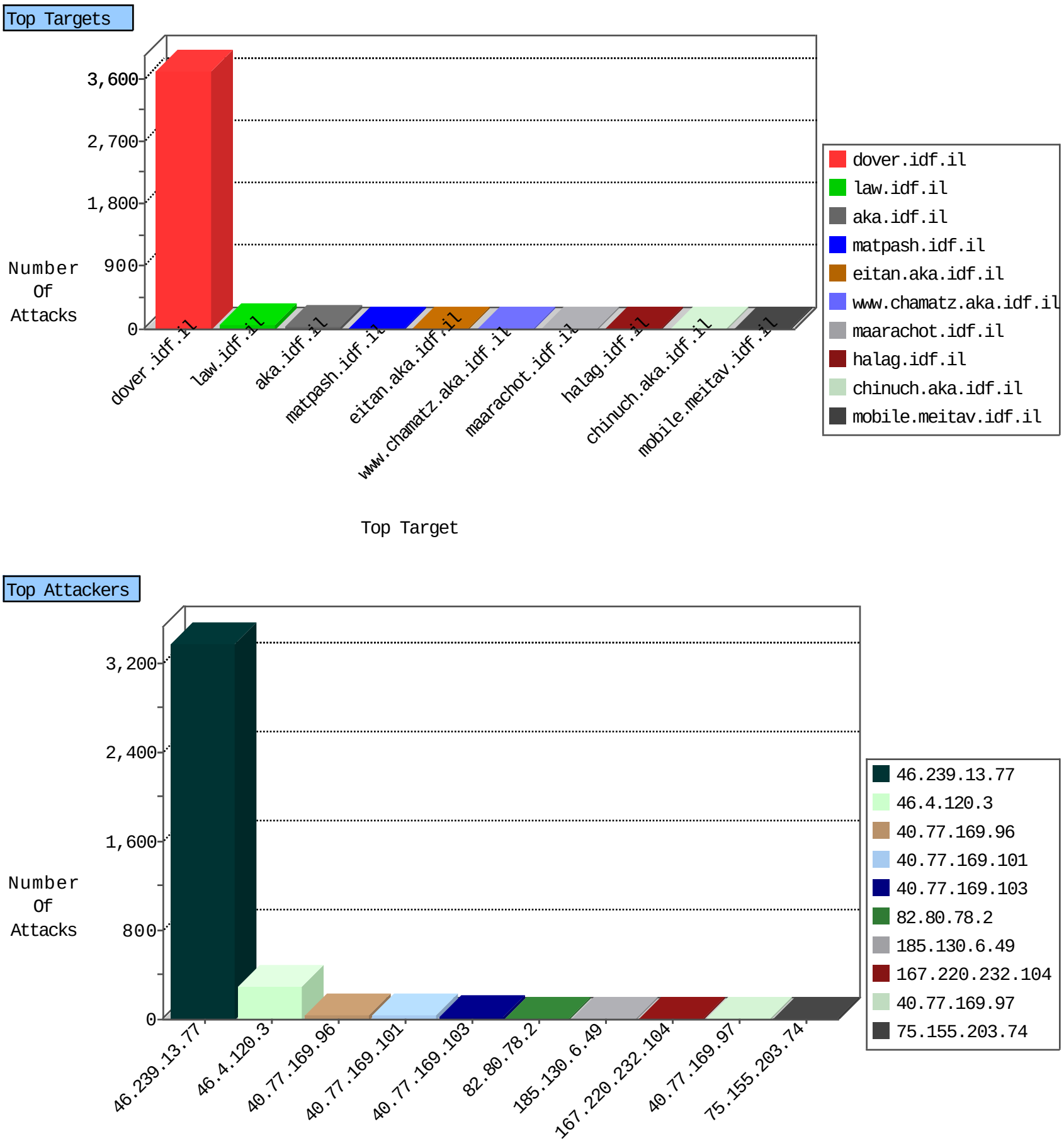
08-27-2016-07:04:00 to 08-27-2016-08:04:00

IDF Under Attack Daily Report



08-27-2016-07:04:00 to 08-27-2016-08:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	7
82.80.78.2	Israel	147.237.77.226	www.chamatz.aka.idf.il	Black List	drop	6
204.42.253.132	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
66.240.236.119	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1

08-27-2016-07:04:00 to 08-27-2016-08:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.120.3	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	219
46.4.120.3	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	37
46.4.120.3	Germany	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	19
46.4.120.3	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	7
46.4.120.3	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	4
46.4.120.3	Germany	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	3
46.4.120.3	Germany	147.237.77.226	www.chamatz.aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
46.4.120.3	Germany	147.237.76.147	chinuch.aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
46.4.120.3	Germany	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Permit	2
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
151.80.31.182	France	147.237.72.166	aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.51.25	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	1

08-27-2016-07:04:00 to 08-27-2016-08:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
146.200.158.162	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
27.254.130.46	147.237.76.198	Thailand	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
104.197.206.193	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 3072	1
27.254.130.46	147.237.76.42	Thailand	refuah.idf.il	ET SCAN Potential SSH Scan	1
104.197.206.193	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -f -sS	1
27.254.130.46	147.237.0.34	Thailand	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.158	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -f -sS	1
219.87.191.219	147.237.76.38	Taiwan	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 2048	1
219.87.191.219	147.237.0.33	Taiwan	idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -f -sS	1
183.82.106.200	147.237.0.15	India	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
85.113.117.14	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	1
163.172.169.150	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
27.254.130.46	147.237.76.202	Thailand	e.halag.idf.il	ET SCAN Potential SSH Scan	1
123.206.85.139	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
27.254.130.46	147.237.76.197	Thailand	e.himush.idf.il	ET SCAN Potential SSH Scan	1
104.197.206.193	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 2048	1
27.254.130.46	147.237.76.34	Thailand	yohalan.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
219.87.191.219	147.237.76.202	Taiwan	e.halag.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.77.121	Ukraine	e.navy.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
219.87.191.219	147.237.0.35	Taiwan	akaws.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.106.200	147.237.0.15	India	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
163.172.169.150	147.237.8.14	United Kingdom	e.orchot.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
27.254.130.46	147.237.77.19	Thailand	law-forum.idf.il	ET SCAN Potential SSH Scan	1

08-27-2016-07:04:00 to 08-27-2016-08:04:00

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	3285
46.239.13.77	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	100
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	33
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
40.77.169.101	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	12
40.77.169.101	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	8
167.220.232.104	Japan	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
40.77.169.97	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	8
40.77.169.96	United States	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	8
185.130.6.49	Lithuania	147.237.77.74	law.idf.il	drop	SAM rule	drop	6
185.130.6.49	Lithuania	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	6
75.155.203.74	Canada	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
40.77.169.96	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
176.13.13.67	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.46	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	2
188.120.148.243	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.193.108.52	Russian Federation	147.237.77.226	www.chamatz.aka.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
40.77.169.104	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
141.212.121.185	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
106.38.241.105	China	147.237.0.34	tikshuv.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
190.27.240.37	Colombia	147.237.76.86	navy.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

08-27-2016-07:04:00 to 08-27-2016-08:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.28.141.67	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	3
79.179.16.9	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
40.77.169.102	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 40.77.169.102	Block	3
40.77.169.98	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
71.202.16.221	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
157.55.2.142	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.2.182	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.66.109.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
65.55.210.162	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-12847-he/dover.aspx„'"•'¡'ƒ„'„†λ€™„ƒλ¬,λ¢„ €λ„¢„ƒ„'„¢λ,¬„¡„ƒλ€š„,„¯„ƒ„'„†λ€™„ƒ„¢„¢λ€š„¬„…„¡„ƒ„'„¢λ,¬„¡„ƒλ€š„,„¿„…„¡„ƒ„'„¢λ,¬„¡„ƒλ€š„,„½	Block	1
40.77.169.100	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.64.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/smalim/showbig.aspx	Block	1
75.155.203.74	Canada	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
40.77.169.100	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.66.209	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
75.155.203.74	Canada	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
40.77.169.102	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
157.55.39.14	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/shared/usercontrols/trajector/	Block	1
66.249.76.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1884	Block	1
199.30.24.51	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

08-27-2016-07:04:00 to 08-27-2016-08:04:00