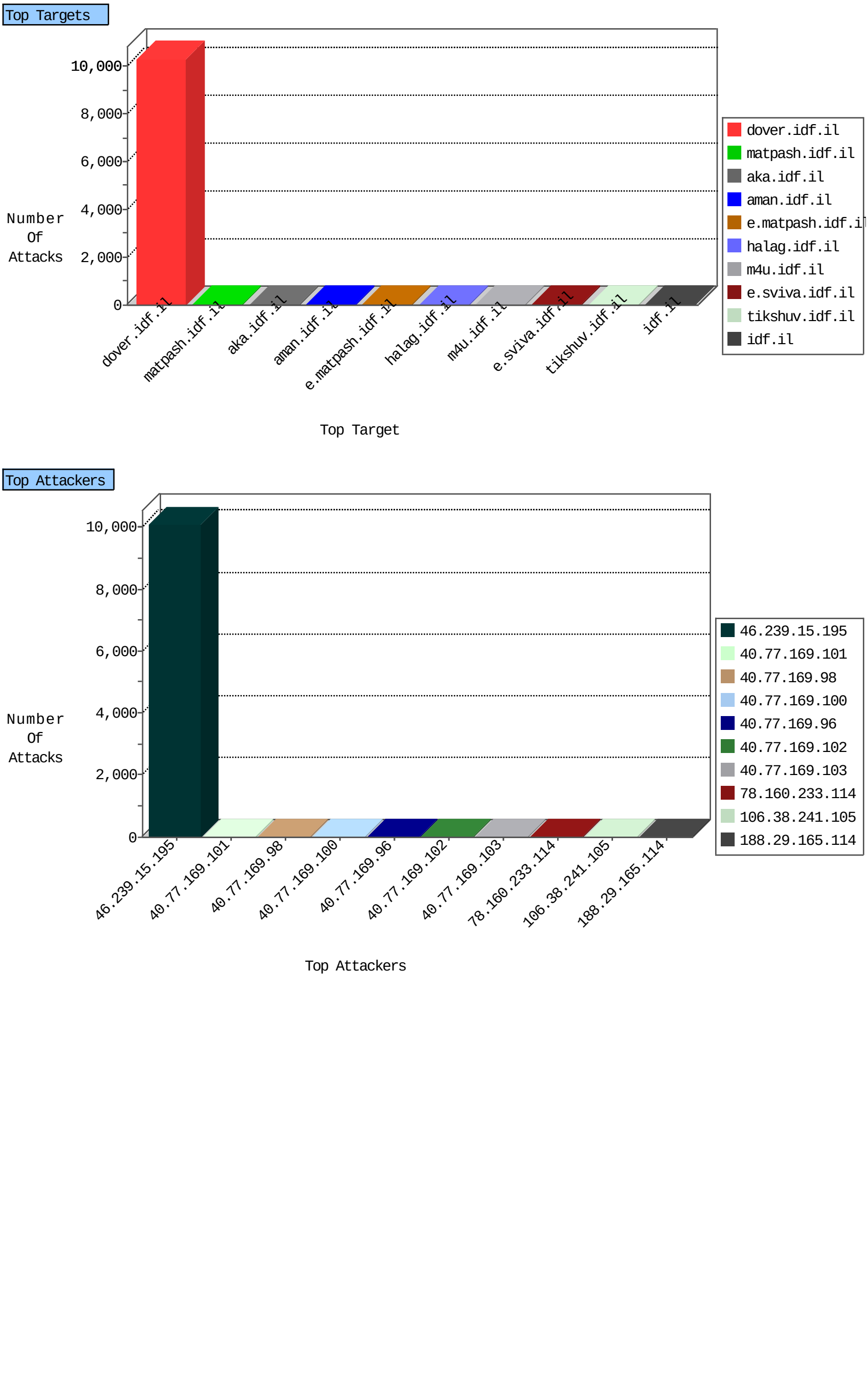
08-28-2016-04:04:06 to 08-28-2016-05:04:06

IDF Under Attack Daily Report



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

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
115.230.125.146	China	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
115.230.125.146	China	147.237.77.216	dover.idf.il	block-sp-traf1	forward	1
123.59.59.52	China	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	1
104.238.184.170	United Kingdom	147.237.76.31	nakchal.idf.il	Black List	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
46.165.197.141	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.130	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
46.165.197.142	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

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

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
188.19.144.78	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.169.150	147.237.72.217	United Kingdom	e.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.169.150	147.237.72.156	United Kingdom	aman.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.155	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.50	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
210.121.12.25	147.237.0.33	Korea, Republic of	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
201.238.202.219	147.237.76.200	Chile	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
176.107.177.47	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.72.166	United Kingdom	aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
123.100.170.134	147.237.0.19	Korea, Republic of	madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.155	147.237.76.196	Ukraine	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
211.141.78.56	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
209.66.70.253	147.237.77.74	United States	law.idf.il	Tehila - Perl LWP with fake user agent	1

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

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	9917
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	200
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	19
40.77.169.100	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	18
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
78.160.233.114	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
40.77.169.101	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	11
188.29.165.114	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
40.77.169.103	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
40.77.169.103	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
31.43.138.18	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop		drop	4
40.77.169.101	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
106.38.241.105	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	2
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
40.77.169.104	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
108.61.123.83	France	147.237.0.33	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	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
128.232.110.28	United Kingdom	147.237.76.34	yohalan.idf.il	drop		drop	1
106.38.241.105	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
74.82.47.34	United States	147.237.0.200	m4u.idf.il	drop		drop	1
40.77.169.102	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
74.129.172.229	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
106.38.241.105	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
45.56.74.212	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	7
131.253.27.21	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	4
131.253.27.7	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
204.79.180.196	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
68.180.230.171	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.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
207.46.13.78	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.230.171	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
148.251.2.180	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/iturim/asp/displayonesoldier.asp	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
87.68.35.41	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/1110-he/tikshuv.asp	Block	1
5.22.135.215	Israel	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
185.89.216.225	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
108.84.128.30	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
5.22.135.215	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
185.89.216.232	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1