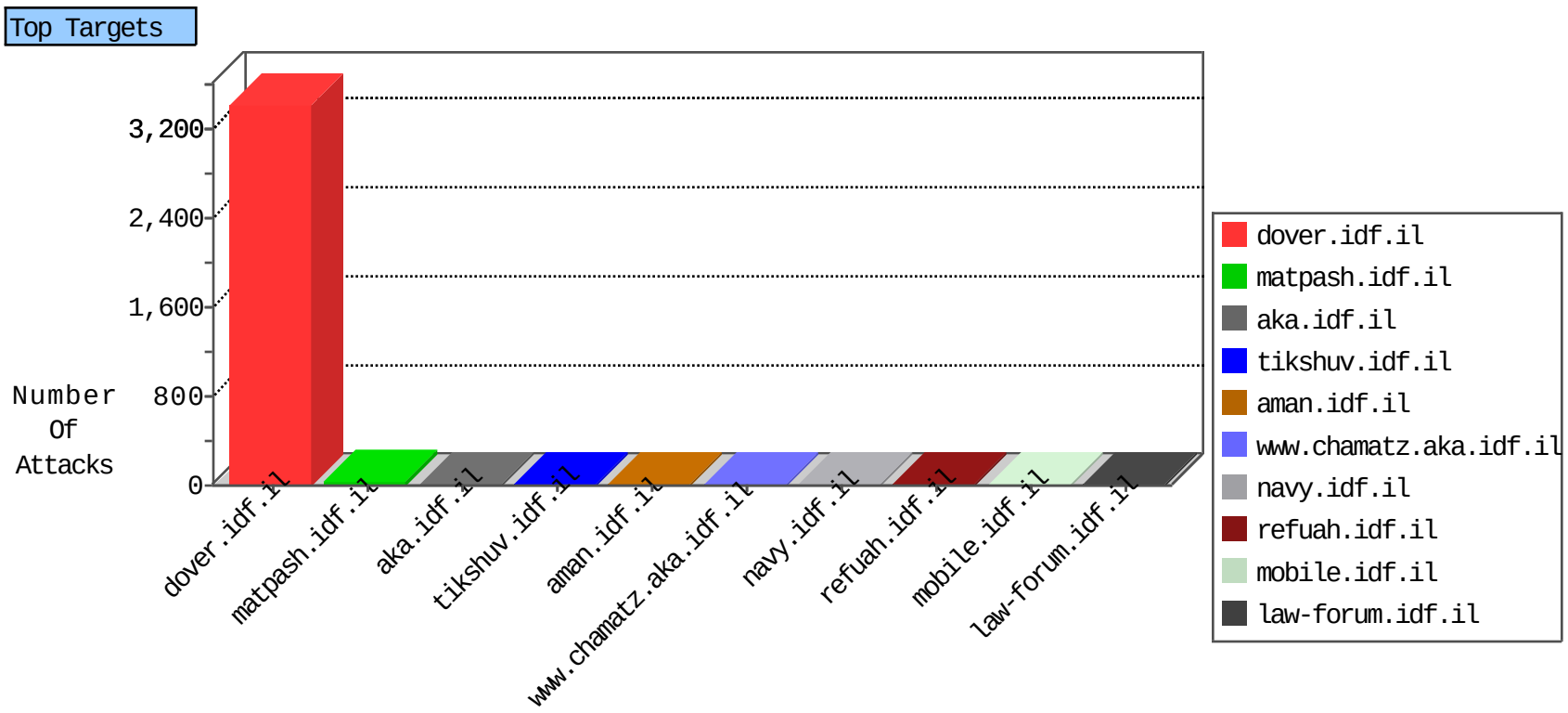
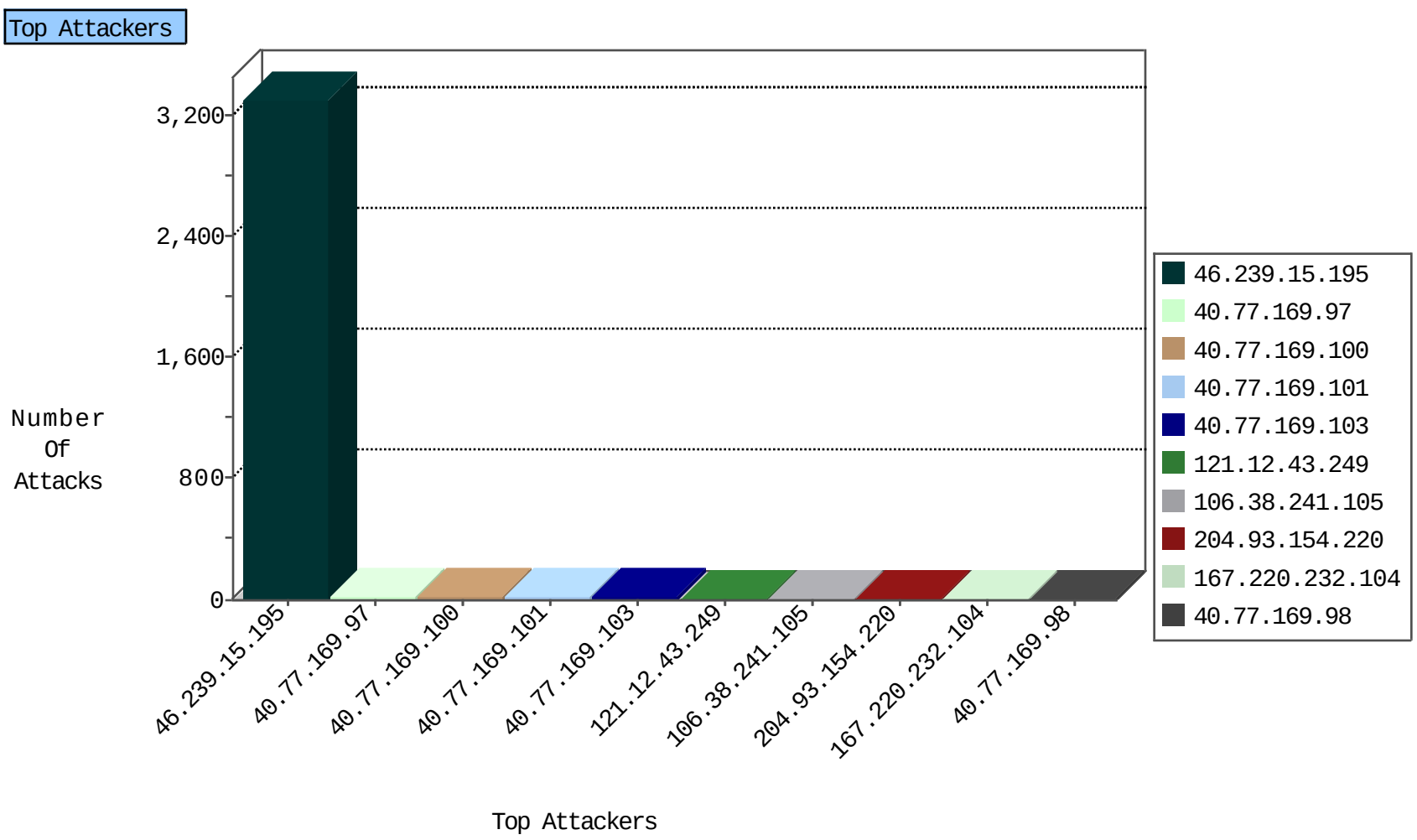
08-28-2016-02:04:07 to 08-28-2016-03:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-28-2016-02:04:07 to 08-28-2016-03:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.220	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	186
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
82.80.78.2	Israel	147.237.77.226	www.chamatz.aka.idf.il	Black List	drop	2

08-28-2016-02:04:07 to 08-28-2016-03:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
121.12.43.249	China	147.237.0.34	tikshuv.idf.il	C1000076: HTTP: Trying to locate existing FCKeditor	Permit	10

08-28-2016-02:04:07 to 08-28-2016-03:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.32.179.28	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.169.150	147.237.72.156	United Kingdom	aman.idf.il	ET SCAN NMAP -sS window 1024	1
125.77.28.26	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
211.141.78.56	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
211.141.78.56	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.141.78.56	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.149	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
183.129.160.229	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
125.77.28.26	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
5.255.82.56	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
211.141.78.56	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.141.78.56	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
211.141.78.56	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.201.225.149	147.237.77.226	Ukraine	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1

08-28-2016-02:04:07 to 08-28-2016-03:04:07

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	3157
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	150
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
40.77.169.97	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	20
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
167.220.232.104	Japan	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
40.77.169.98	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	7
40.77.169.102	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	6
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
185.6.58.1	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.9.122.203	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
40.77.169.104	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
176.13.1.223	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.178.216.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
40.77.169.101	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
40.77.169.98	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
106.38.241.105	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	2
106.38.241.105	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	2
40.77.169.100	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
185.6.58.1	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.101	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
176.13.224.225	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
137.117.168.203	United States	147.237.0.33	idf.il	drop		drop	1
176.13.245.216	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
137.117.168.203	United States	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
106.38.241.105	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
40.77.169.103	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
109.253.130.198	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1

08-28-2016-02:04:07 to 08-28-2016-03:04:07

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	4
79.242.106.152	Germany	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/general.aspx	Block	3
109.66.153.139	Israel	147.237.77.243	mobile.idf.i	Distributed Suspicious Response Code	Block	2
207.46.13.84	United States	147.237.76.42	refuah.idf.i	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
77.139.26.28	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
2.55.170.241	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
119.229.22.56	Japan	147.237.0.34	tikshuv.idf.	Unauthorized URL Access to www.tikshuv.idf.il/wp-login.php	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.i	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	1
213.8.204.64	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
5.22.135.109	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
121.12.43.249	China	147.237.0.34	tikshuv.idf.	Admin Blocking	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
213.8.204.64	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
82.166.228.10	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
176.35.222.2	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.106	Block	1
46.121.63.50	Israel	147.237.76.42	refuah.idf.i	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/1740.png	Block	1
204.79.180.163	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1
66.249.76.117	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20063-he/idfgdover.aspx	Block	1
2.53.165.40	Israel	147.237.77.243	mobile.idf.i	Distributed Suspicious Response Code	Block	1
119.229.22.56	Japan	147.237.0.34	tikshuv.idf.	PHP Attempt	Block	1
46.229.164.102	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/robots.txt	Block	1

08-28-2016-02:04:07 to 08-28-2016-03:04:07