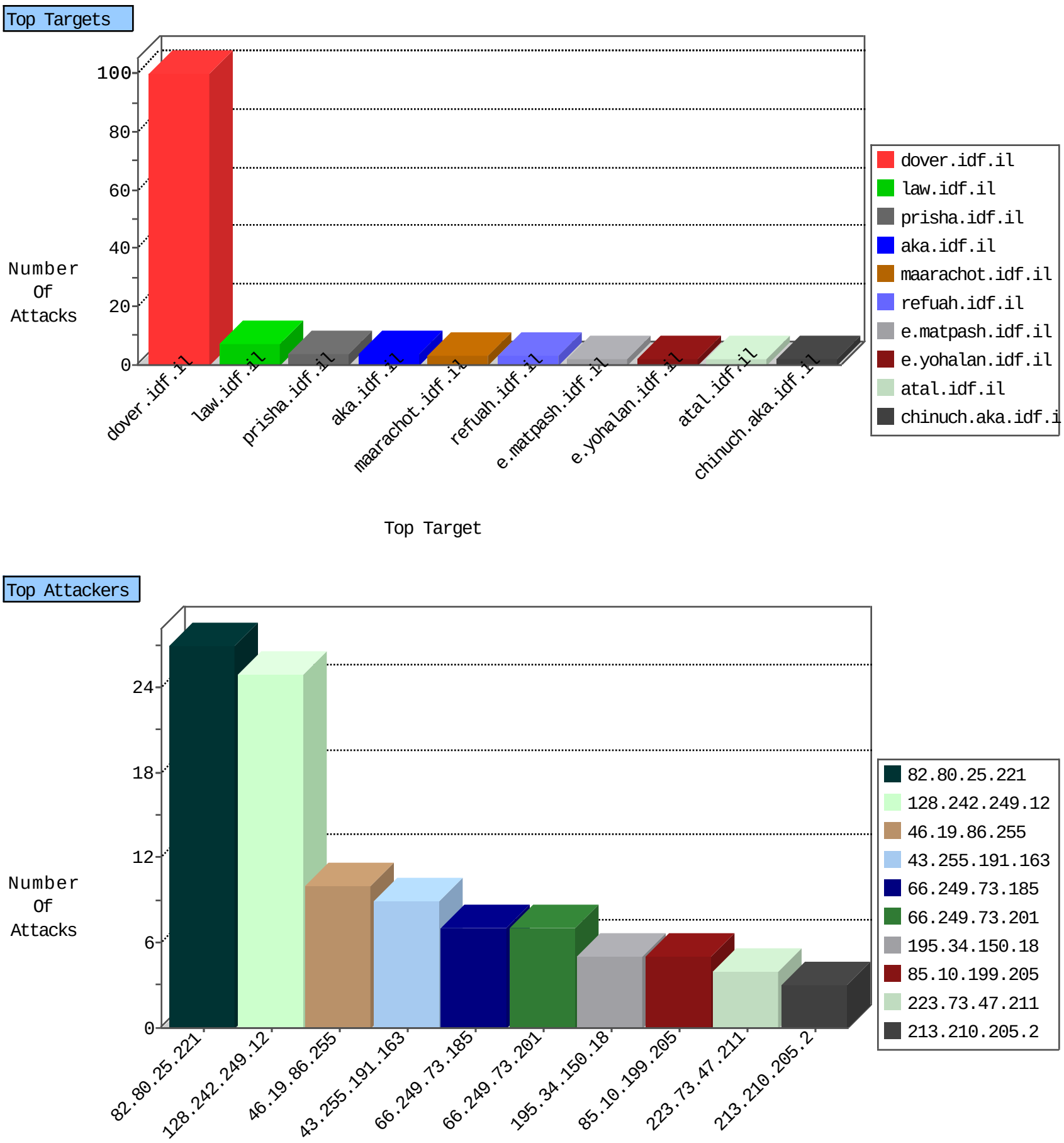
04-25-2015-05:03:02 to 04-25-2015-06:03:02

IDF Under Attack
04-25-2015-05:03:02



04-25-2015-05:03:02 to 04-25-2015-06:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
23.94.144.50	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
222.148.170.131	Japan	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

04-25-2015-05:03:02 to 04-25-2015-06:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	25
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	1
61.41.4.6	Korea, Republic of	147.237.77.74	law.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
85.25.103.50	Germany	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1

04-25-2015-05:03:02 to 04-25-2015-06:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	27
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.69.63	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
23.254.132.248	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -f -sS	1
61.240.144.64	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
213.210.205.2	Saudi Arabia	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.163	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
213.210.205.2	Saudi Arabia	147.237.77.205	prisha.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.163	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
85.10.199.205	Germany	147.237.77.233	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.163	Japan	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
85.10.199.205	Germany	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.163	Japan	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
85.10.199.205	Germany	147.237.8.24	e.lifestyle.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
23.254.132.248	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
213.210.205.2	Saudi Arabia	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.163	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
85.10.199.205	Germany	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
43.255.191.163	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
85.10.199.205	Germany	147.237.8.45	e.eitan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
23.254.132.248	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 2048	1

04-25-2015-05:03:02 to 04-25-2015-06:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.86.255	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
186.31.188.11	Colombia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
37.247.36.75	Netherlands	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
95.173.190.4	Turkey	147.237.76.147	chinuch.aka.idf.il		drop	drop	1
207.241.226.169	United States	147.237.72.166	aka.idf.il	SAM rule	drop	drop	1
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
95.173.190.4	Turkey	147.237.76.198	e.yohalan.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
140.139.231.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
72.47.132.65	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
162.216.13.2	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
82.145.216.128	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

04-25-2015-05:03:02 to 04-25-2015-06:03:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	7
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	7
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	3
223.73.47.211	China	147.237.77.74	law.idf.il	PHP Attempt	Block	3
91.200.12.11	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
66.249.79.112	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/m/	Block	1
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2004/march/22a.stm	Block	1
116.0.0.218	Indonesia	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
223.73.47.211	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/ckeditor/ckfinder/core/connector/aspx/connector.aspx	Block	1
66.249.69.36	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
188.165.15.13	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.13	Block	1
74.82.47.4	United States	147.237.76.39	mobile.meitav.idf.i	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.69.84	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/paratroopers	Block	1
66.249.75.43	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
79.178.184.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.92	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1

04-25-2015-05:03:02 to 04-25-2015-06:03:02