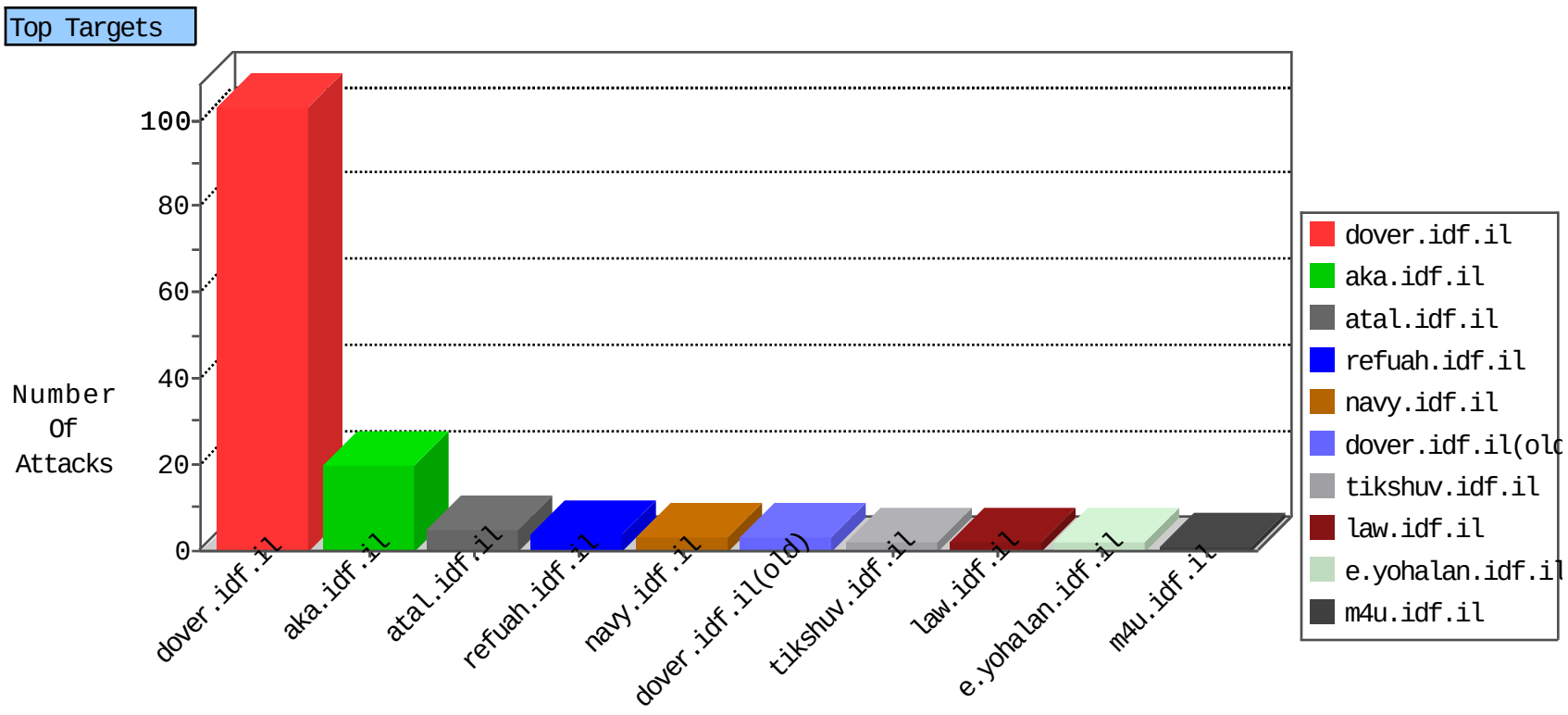
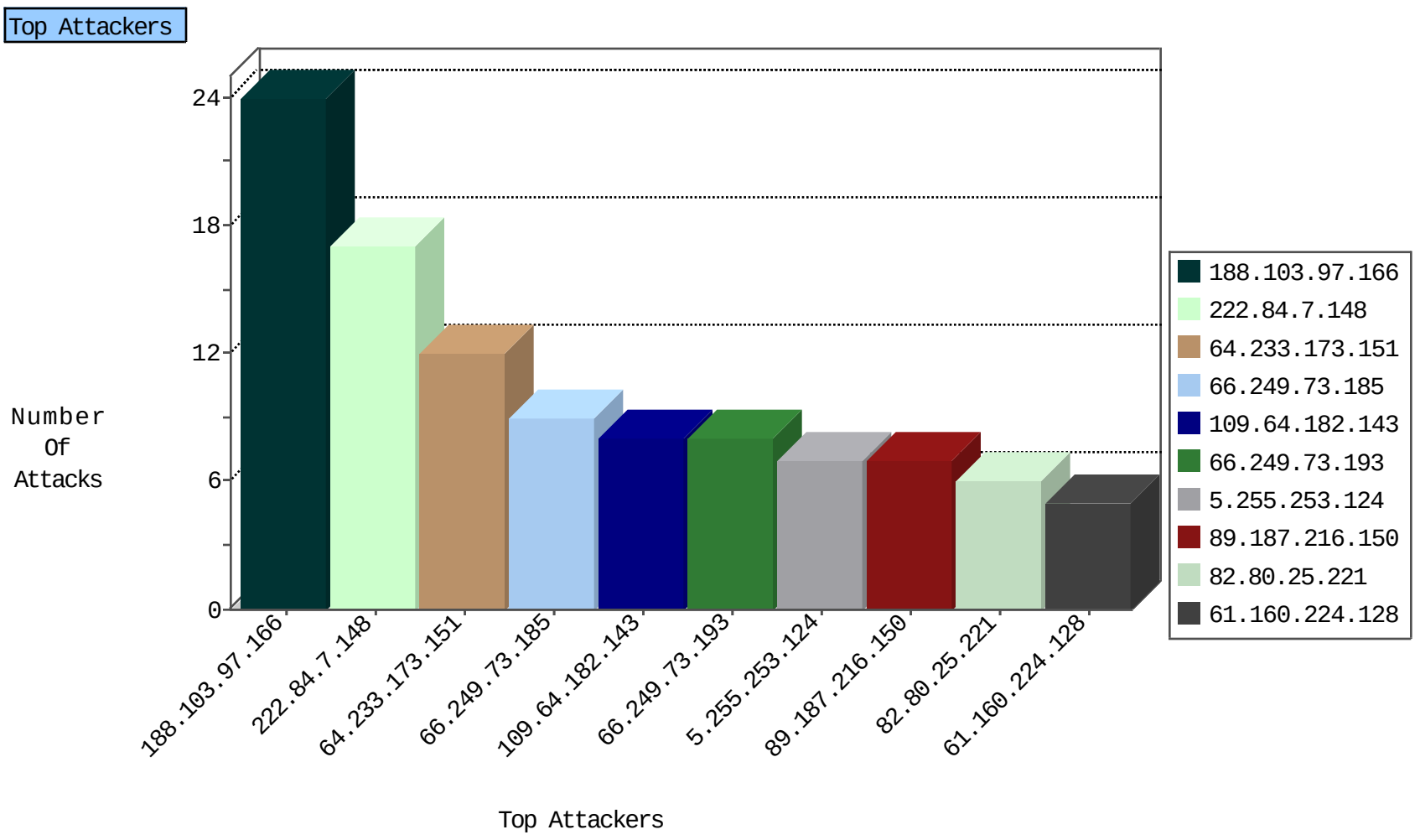
04-25-2015-07:03:02 to 04-25-2015-08:03:02

IDF Under Attack
04-25-2015-07:03:02

Top Targets



Top Attackers



04-25-2015-07:03:02 to 04-25-2015-08:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
58.153.235.110	Hong Kong	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

04-25-2015-07:03:02 to 04-25-2015-08:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
198.20.69.98	United States	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
163.47.14.86	Japan	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-25-2015-07:03:02 to 04-25-2015-08:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
222.84.7.148	China	147.237.72.166	aka.idf.il	SQL Injection - Select From	17
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
64.233.173.161	United States	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
64.122.98.58	United States	147.237.77.179	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
202.71.25.29	India	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
91.224.132.118	Russian Federation	147.237.0.200	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
81.200.91.2	Russian Federation	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
61.240.144.66	China	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.128	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.128	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
202.71.25.29	India	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
81.200.91.2	Russian Federation	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

04-25-2015-07:03:02 to 04-25-2015-08:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
188.103.97.166	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	24
64.233.173.151	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
109.64.182.143	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	8
89.187.216.150	Lebanon	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	7
66.249.73.185	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.73.193	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.86.77	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
54.72.73.168	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
207.46.13.52	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1

04-25-2015-07:03:02 to 04-25-2015-08:03:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	6
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	3
187.45.240.69	Brazil	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 187.45.240.69	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
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	2
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	2
165.124.164.167	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	2
66.249.75.66	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
52.4.251.232	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arafat/terrorism2/english/main_index.stm	Block	1
178.19.104.138	Poland	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
69.30.240.46	United States	147.237.72.167	ishurim.aka.idf.i	Illegal HTTP Version	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info03.stm	Block	1
157.55.39.24	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
66.249.75.72	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/mobile/	Block	1
54.166.33.25	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
217.12.202.39	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.79	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/467-he/patzar.aspx	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//	Block	1
54.176.35.127	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
188.143.232.40	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.40	Block	1
74.82.47.2	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/smalim/&sa=u&ei=rtowtn-eh86con2n-jsc&ved=0cauqfjaa&usg=afqjcnfq_09hupqmgnkek7wo5wtfda-oqg	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/scriptresource.axd	Block	1
66.249.64.64	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//938-he/refuah.aspx	Block	1
188.143.232.40	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
84.228.16.124	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/undefined	Block	1
66.249.75.5	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
31.193.51.80	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//scriptresource.axd	Block	1
66.249.64.83	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/m/	Block	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.1	Block	1
109.253.134.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

04-25-2015-07:03:02 to 04-25-2015-08:03:02