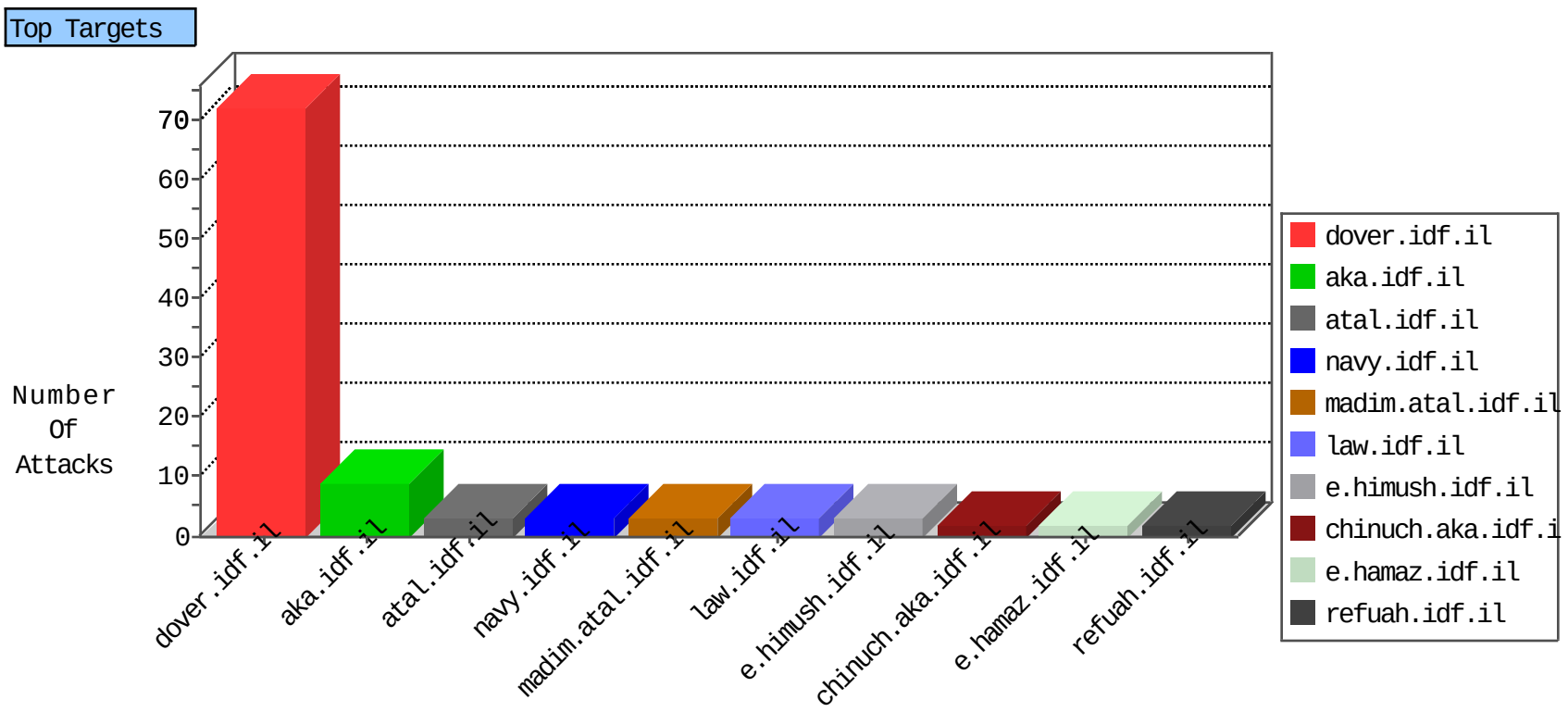
04-25-2015-08:03:06 to 04-25-2015-09:03:06

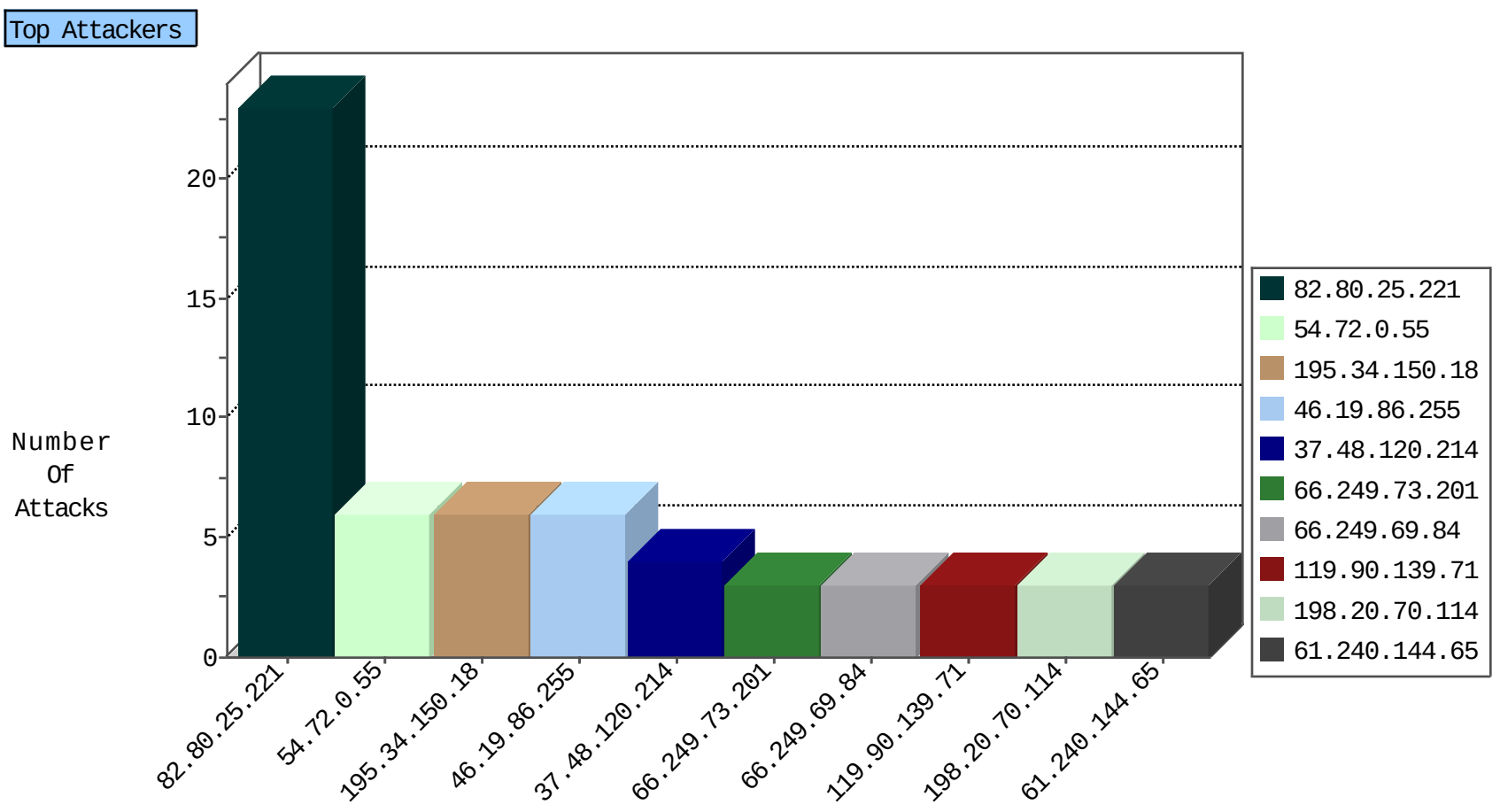
IDF Under Attack
04-25-2015-08:03:06

Top Targets



Top Target

Top Attackers



Top Attackers

04-25-2015-08:03:06 to 04-25-2015-09:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.18	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	376
112.144.116.198	Korea, Republic of	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	2

04-25-2015-08:03:06 to 04-25-2015-09:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
218.30.103.52	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
85.25.103.50	Germany	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1

04-25-2015-08:03:06 to 04-25-2015-09:03:06

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	23
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.69.84	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.65	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
216.14.93.126	United States	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.85.232	Netherlands	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
119.90.139.71	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
111.203.22.57	China	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
101.226.2.99	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243		147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.203.126	Israel	147.237.72.156	aman.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
218.77.79.43	China	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
216.14.93.126	United States	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -f -sS	1
5.255.85.232	Netherlands	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 3072	1
119.90.139.71	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
119.90.139.71	China	147.237.0.19	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
101.226.2.99	China	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
82.117.208.243		147.237.76.176	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1

04-25-2015-08:03:06 to 04-25-2015-09:03:06

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	6
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
84.108.172.65	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
75.126.221.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
176.12.150.83	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
212.174.166.140	Turkey	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

04-25-2015-08:03:06 to 04-25-2015-09:03:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	3
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	2
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	2
46.117.152.129	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general	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	Unauthorized URL Access to www.idf.il/newsite/english/0223-2.stm	Block	1
79.178.203.131	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.184	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
184.105.139.68	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//newsite/english/main.stm	Block	1
85.65.2.106	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.69.84	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/935	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
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1106-6.stm	Block	1
66.249.75.23	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
37.16.72.139	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/map.stm	Block	1
87.69.127.213	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
188.165.15.13	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/roshhamas.stm	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/tizmoret/	None	1
66.249.75.64	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/m/	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/edim/fund/×³Ö³Æ'Ö¶â€™Ö³â€š Ö²Â¯Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â½×³Ö³Æ'Ö¶â€™Ö³â€š Ö²Â¯Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â½×³Â§×³Ö³Æ'Ö¶â€™Ö³â€š Ö²Â¯Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â½×³Ö³Æ'Ö¶â€™Ö³â€š Ö²Â¯Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â¿Ö³Æ'×'â,¬ÂšÖ³â€šÖ²Â½	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//938-he/refuah.aspx	Block	1
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	1
198.23.155.121	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18822-en	Block	1
66.249.75.74	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
62.219.62.57	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-16655-he/kkkkkkk=0c219c5dkkkkkkk_0c219c5d	Block	1
68.180.228.59	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1

04-25-2015-08:03:06 to 04-25-2015-09:03:06