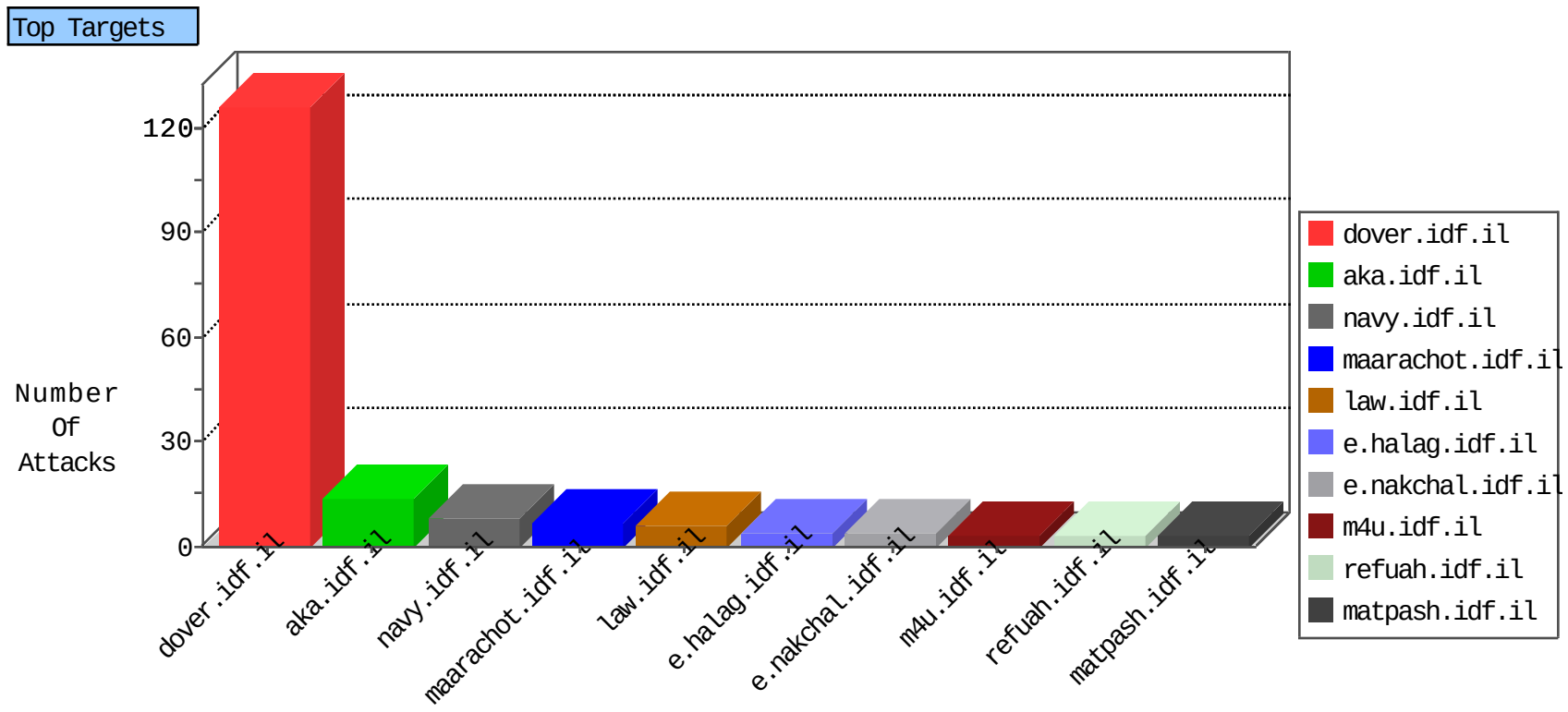
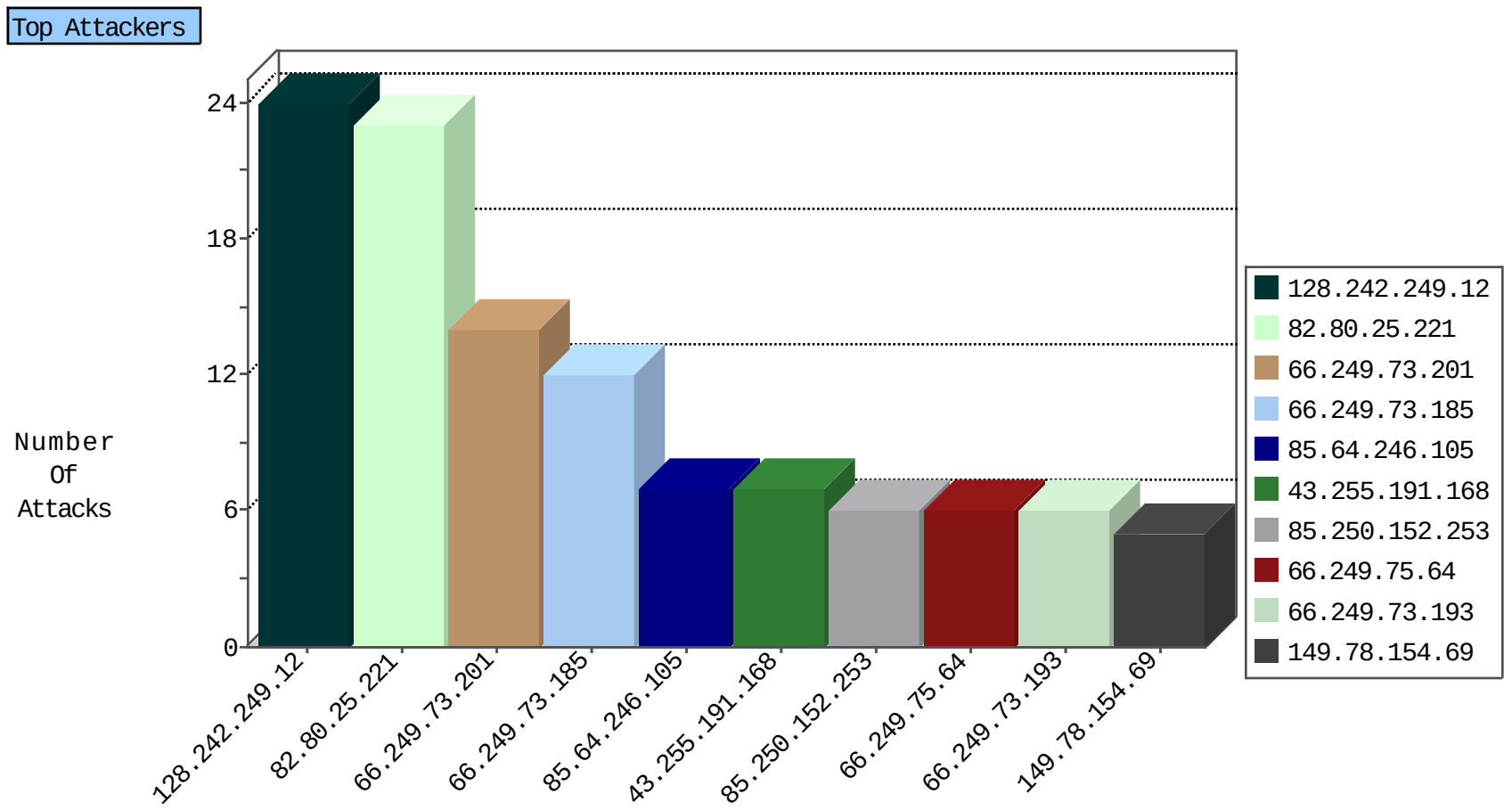
04-25-2015-01:03:07 to 04-25-2015-02:03:07

IDF Under Attack
04-25-2015-01:03:07

Top Targets



Top Attackers



04-25-2015-01:03:07 to 04-25-2015-02:03:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.100	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	2569
220.181.108.90	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	398
182.92.223.10	China	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

04-25-2015-01:03:07 to 04-25-2015-02:03:07

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	24
198.20.69.98	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
174.48.88.221	United States	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.165.200	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
198.27.65.39	Canada	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
85.25.103.50	Germany	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1

04-25-2015-01:03:07 to 04-25-2015-02:03:07

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
66.249.75.64	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
128.30.52.71	United States	147.237.76.86	navy.idf.il	Tehila - Perl LWP with fake user agent	2
50.252.197.194	United States	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.168	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
114.112.96.133	China	147.237.76.34	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.168	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
61.16.232.231	India	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 4096	1
50.252.197.194	United States	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
50.252.197.194	United States	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.168	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
212.47.236.90	France	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.168	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.168	Japan	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
91.238.134.92	Poland	147.237.77.19	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.132.118	Russian Federation	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1

04-25-2015-01:03:07 to 04-25-2015-02:03:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.73.201	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
85.250.152.253	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	6
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
149.78.154.69	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
139.228.163.26	Indonesia	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
207.46.13.1	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
174.57.68.49	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
128.252.79.205	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
184.100.232.198	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
70.184.126.173	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
54.72.0.55	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
108.59.253.71	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
207.46.13.95	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
185.61.49.2		147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
78.55.219.216	Germany	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
62.210.189.96	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
188.165.15.13	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
174.48.88.221	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1

04-25-2015-01:03:07 to 04-25-2015-02:03:07

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	8
85.64.246.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	7
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	6
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	6
91.200.12.11	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	2
188.165.15.13	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.13	Block	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	Block	2
5.35.247.94	Germany	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 5.35.247.94	Block	2
46.119.113.155	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	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
5.79.73.245	Netherlands	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
180.76.4.168	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
46.121.244.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
37.142.236.254	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
52.6.31.228	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-6857-he/	Block	1
2.54.164.163	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
93.172.223.254	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.210	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
188.165.15.13	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0731-1.stm	Block	1
68.180.228.232	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/asp/displayallsoliders.asp	Block	1
66.249.69.33	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
109.64.11.221	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/894-en	Block	1
66.249.75.58	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
207.46.13.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13807-he/dov	Block	1
5.35.247.94	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/homepage/homepage.aspx/webresource.axd	Block	1
134.249.53.8	Ukraine	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//	Block	1
66.249.75.59	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
46.119.113.155	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-11442-en/	Block	1

04-25-2015-01:03:07 to 04-25-2015-02:03:07