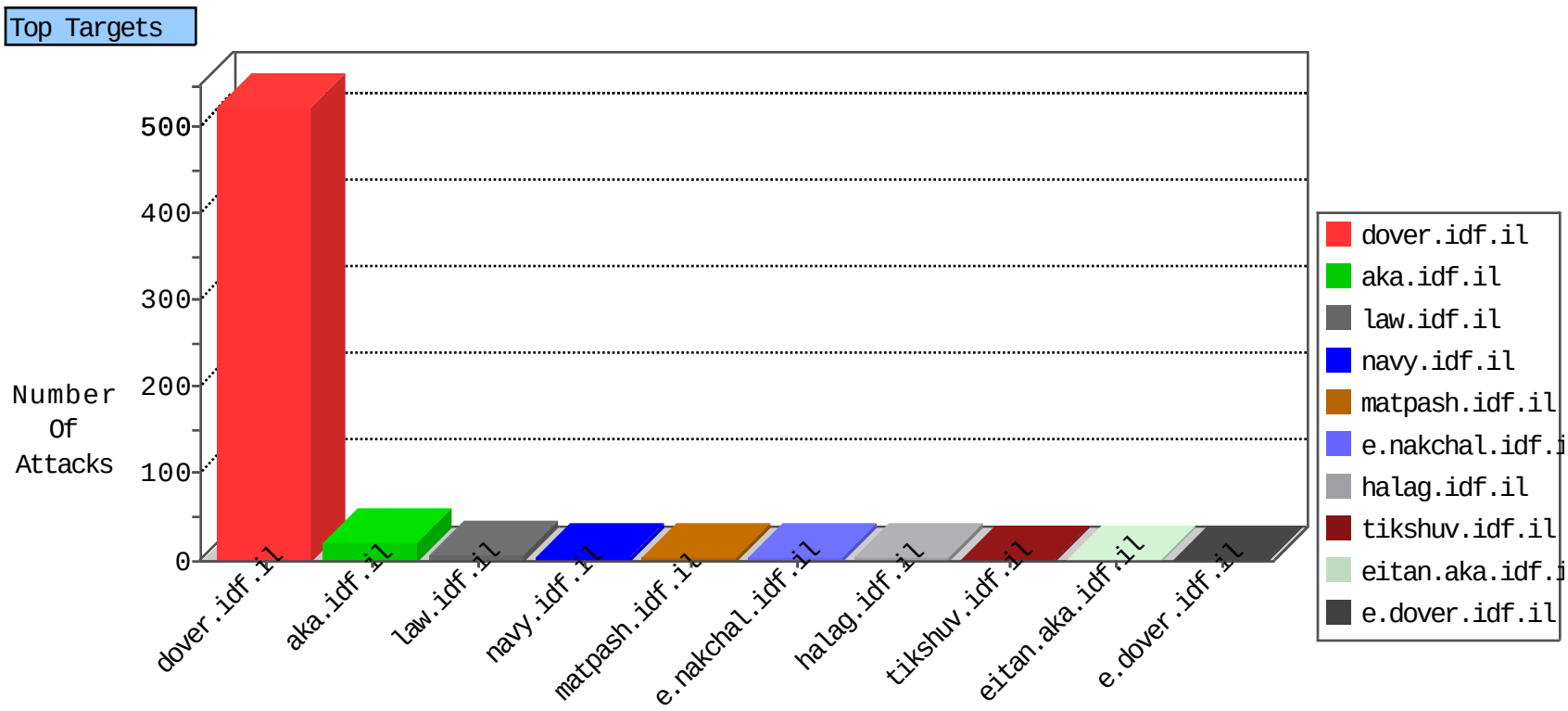
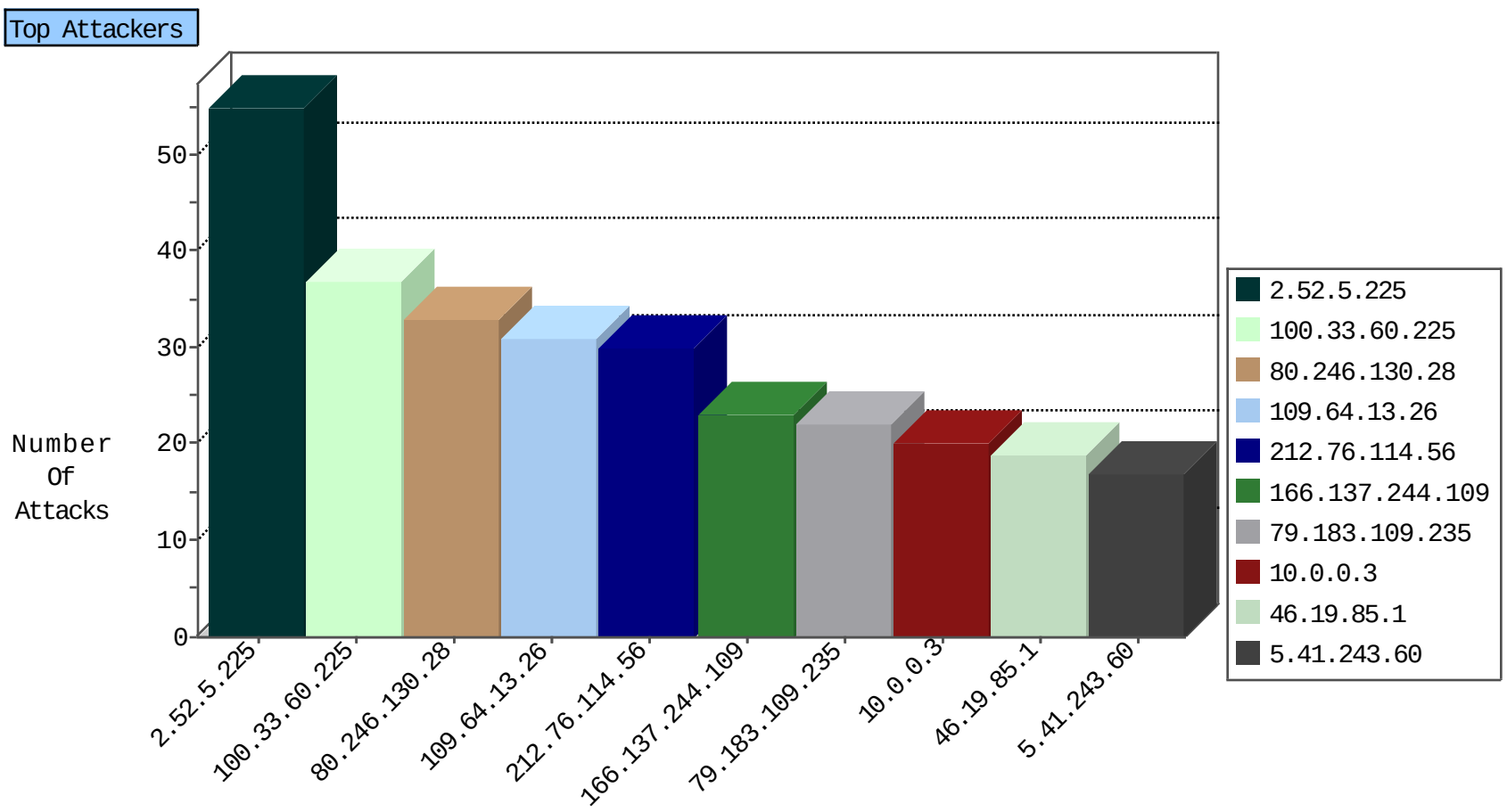
04-24-2015-00:03:01 to 04-24-2015-01:03:01

IDF Under Attack
04-24-2015-00:03:01

Top Targets



Top Attackers



04-24-2015-00:03:01 to 04-24-2015-01:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.83	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	3279
195.34.150.18	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2861
10.0.0.3		147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	20
89.139.170.127	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
79.6.156.128	Italy	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
31.210.186.176	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
46.121.237.166	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

04-24-2015-00:03:01 to 04-24-2015-01:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
89.138.55.238	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1

04-24-2015-00:03:01 to 04-24-2015-01:03:01

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	7
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
37.8.4.131	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	ET SCAN NMAP -sA (2)	2
109.65.55.86	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
79.177.112.168	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
104.167.96.44		147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 2048	1
46.19.86.51	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
104.167.96.44		147.237.77.234	halag.idf.il	ET SCAN NMAP -f -sS	1

04-24-2015-00:03:01 to 04-24-2015-01:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
2.52.5.225	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	55
100.33.60.225	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	37
80.246.130.28	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	33
109.64.13.26	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	31
212.76.114.56	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	30
166.137.244.109	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	23
79.183.109.235	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	22
46.19.85.1	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	18
5.41.243.60	Romania	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	17
79.179.19.34	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	15
2.54.3.140	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	11
197.83.230.214	South Africa	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	10
176.12.144.224	Israel	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
79.179.48.49	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
157.55.39.59	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
109.253.132.123	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
212.76.127.44	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	5
85.64.200.240	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
94.101.4.225	Finland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
85.65.11.33	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
5.102.198.105	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
2.54.1.26	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
46.19.85.234	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	4
89.138.240.45	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
46.19.86.51	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
212.76.127.111	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
194.215.240.253	Finland	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
87.68.214.121	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
79.6.156.128	Italy	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
109.67.194.209	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
212.150.214.90	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
95.86.75.237	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
85.65.25.192	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
79.183.112.72	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
2.54.54.84	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
46.116.184.6	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
37.48.120.214	Netherlands	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	3
64.12.253.130	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
46.19.86.76	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
79.182.5.9	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
80.246.133.221	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
2.54.27.76	Israel	147.237.77.216	dover.idf.i	Invalid ACK number	Bad TCP sequence	monitor	2
66.249.93.160	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
46.19.86.111	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
70.73.229.206	Canada	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
82.205.114.93	Palestinian Territory, Occupied	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
2.54.27.76	Israel	147.237.77.216	dover.idf.i	Invalid sequence number	Bad TCP sequence	monitor	2
212.199.182.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2

04-24-2015-00:03:01 to 04-24-2015-01:03:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
5.29.184.33	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
46.119.113.155	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/	Block	3
128.59.187.171	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/638.pdf	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
79.180.140.183	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//sites/resources/kamlar/styles/import/bottomnavigaton.asp	Block	2
180.76.4.54	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
82.205.114.93	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//894-ar	Block	1
66.249.65.20	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.79.104	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
2.54.161.154	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
188.165.15.87	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/templatecontrols/news/sip_storage/files/7/1437.pdf/	Block	1
84.109.188.47	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.65.157	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
157.55.39.8	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.28.173.146	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
207.46.13.35	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.35	Block	1
85.250.61.138	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.211	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
157.55.39.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/hativa7/clali.stm	Block	1
212.252.167.214	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/homefront/earth.stm	Block	1
109.65.222.237	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.219	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
166.172.189.153	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
82.205.112.74	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il//894-ar	Block	1
109.186.54.101	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
66.249.73.240	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1

04-24-2015-00:03:01 to 04-24-2015-01:03:01