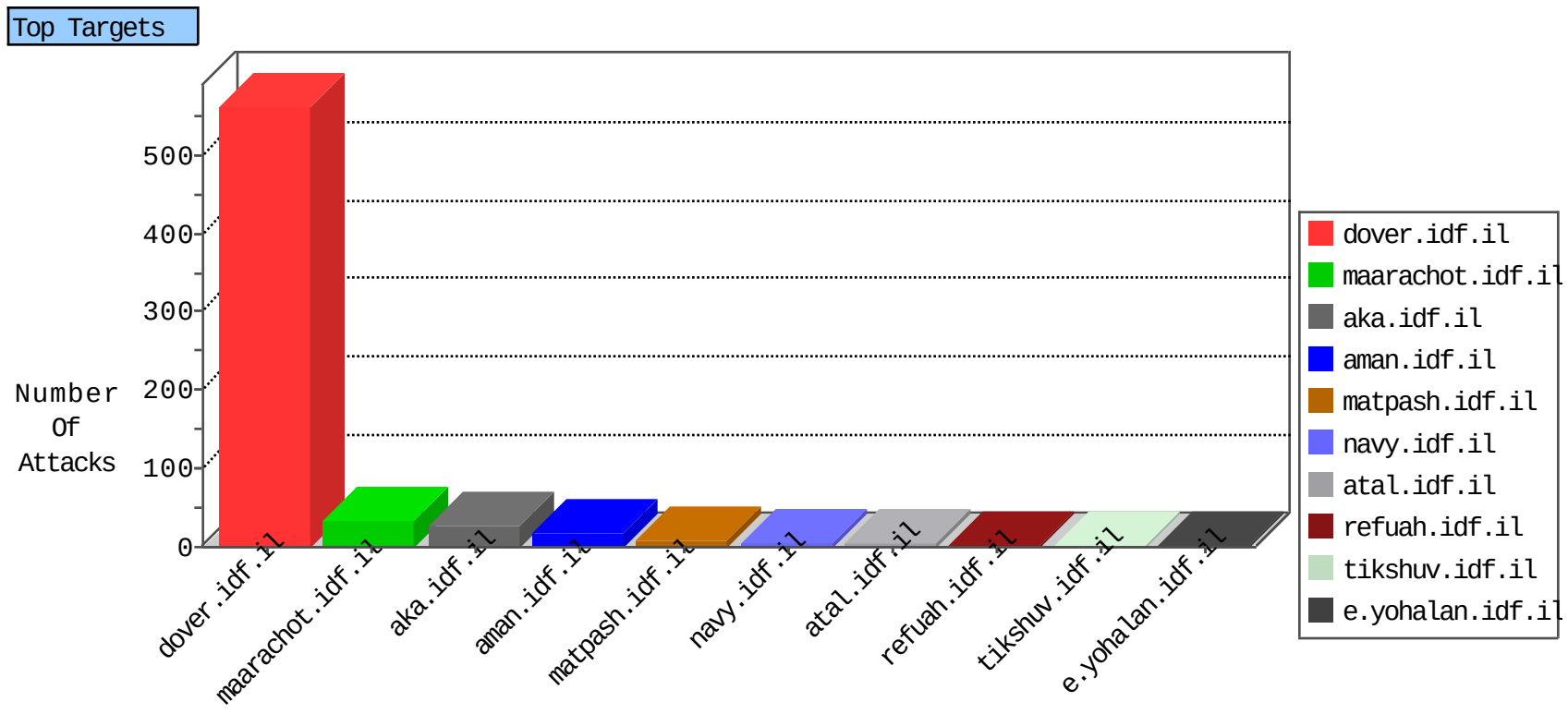
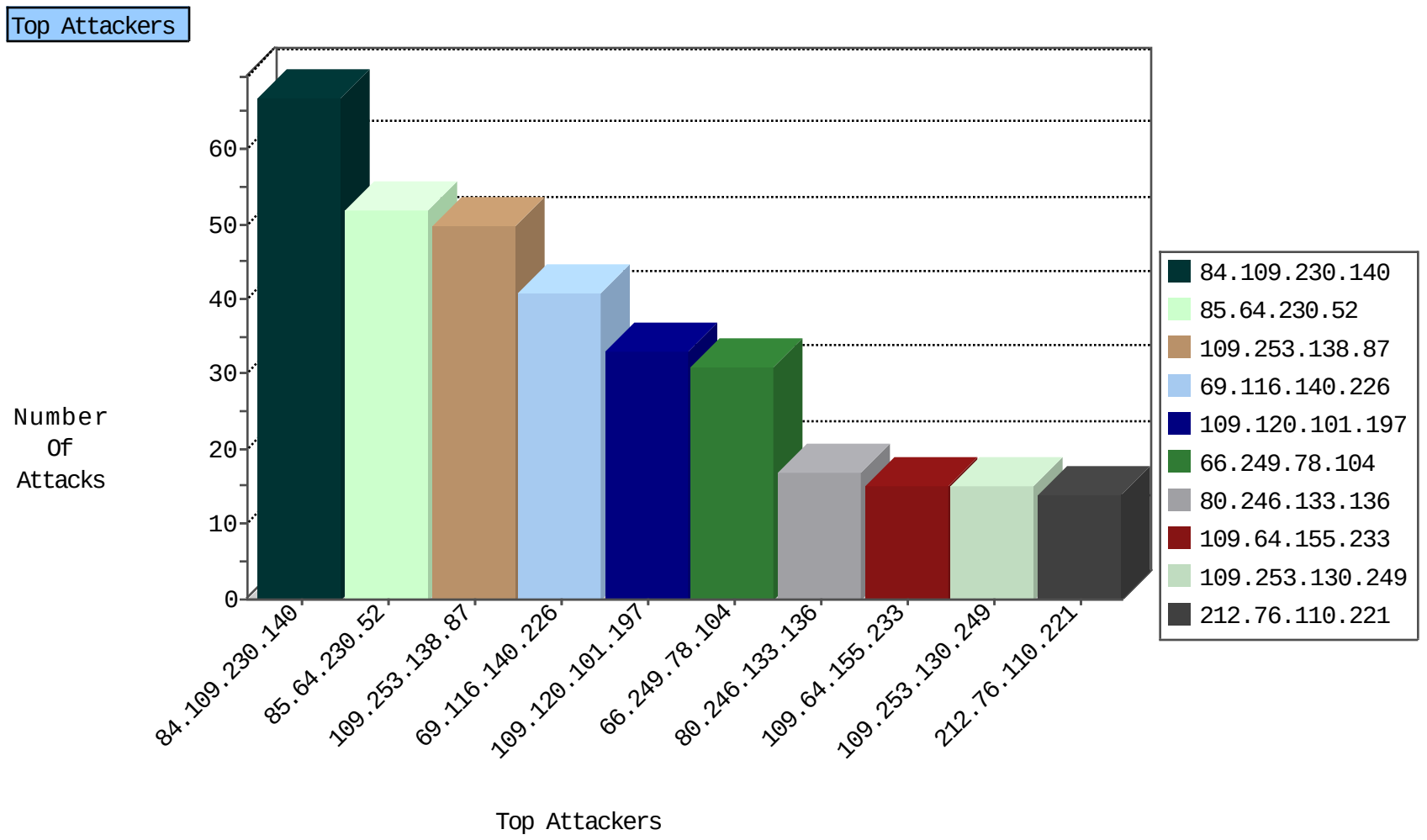
04-23-2015-23:03:04 to 04-24-2015-00:03:04

IDF Under Attack
04-23-2015-23:03:04

Top Targets



Top Attackers



04-23-2015-23:03:04 to 04-24-2015-00:03:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	6197
62.218.31.10	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	787
108.41.12.139	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	622
94.123.152.100	Turkey	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	357
109.64.155.233	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	99
46.19.85.11	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	43
109.64.169.77	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
85.64.230.52	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
85.64.40.210	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
124.232.142.220	China	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

04-23-2015-23:03:04 to 04-24-2015-00:03:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
80.178.15.170	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
93.120.27.62	Romania	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.16	my-kosher-kravi.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
79.182.32.2	Israel	147.237.77.74	law.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1

04-23-2015-23:03:04 to 04-24-2015-00:03:04

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
2.54.28.76	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
114.112.90.54	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
67.50.5.217	United States	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.67	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243		147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
212.47.228.73	France	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1

04-23-2015-23:03:04 to 04-24-2015-00:03:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.109.230.140	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	67
109.253.138.87	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
85.64.230.52	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	50
69.116.140.226	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	41
109.120.101.197	Luxembourg	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
80.246.133.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	17
109.253.130.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
212.76.110.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	14
176.67.58.67	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
62.128.45.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	11
212.199.57.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
2.52.49.65	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
37.26.147.185	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
62.219.154.56	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
109.67.146.61	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
79.177.182.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
46.19.86.125	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
192.118.78.198	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
95.86.112.200	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
176.106.47.98	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
5.28.133.115	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
109.253.156.94	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
80.246.133.206	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
85.250.36.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
80.246.133.218	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
87.69.171.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
85.250.170.32	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
82.205.104.192	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
212.199.205.68	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
85.72.40.4	Greece	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
176.12.136.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.54.159.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.79.58	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
87.68.84.193	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.142.234.106	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
152.201.98.66		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
93.173.231.207	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
176.12.146.62	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
134.191.232.70	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
5.22.130.189	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
46.19.86.245	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
201.6.217.125	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

04-23-2015-23:03:04 to 04-24-2015-00:03:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
79.182.25.73	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
212.76.97.74	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	3
212.76.97.74	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/6_s3_	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
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
164.138.127.138	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
176.106.47.98	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	2
157.55.39.251	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kapatz/	Block	1
46.19.86.56	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
188.120.148.147	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.173	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/mobile/	Block	1
2.54.171.186	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
66.249.64.86	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
188.138.17.205	France	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
157.55.39.81	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.81	Block	1
66.249.65.178	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
5.28.184.122	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
176.10.104.227	Switzerland	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 176.10.104.227	Block	1
79.182.25.73	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
66.249.65.22	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
157.55.39.81	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/ishurim	Block	1
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/english/ie-index02.stm	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arafat/continuation/english/index2.stm	Block	1
176.10.104.227	Switzerland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1043-en/	Block	1
84.108.65.245	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.65.60	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
157.55.39.210	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/sachar	Block	1
66.249.79.96	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19795-he/idfgdover.aspx	Block	1
46.19.86.56	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
98.172.138.85	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.65.152	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/mobile/	Block	1

04-23-2015-23:03:04 to 04-24-2015-00:03:04