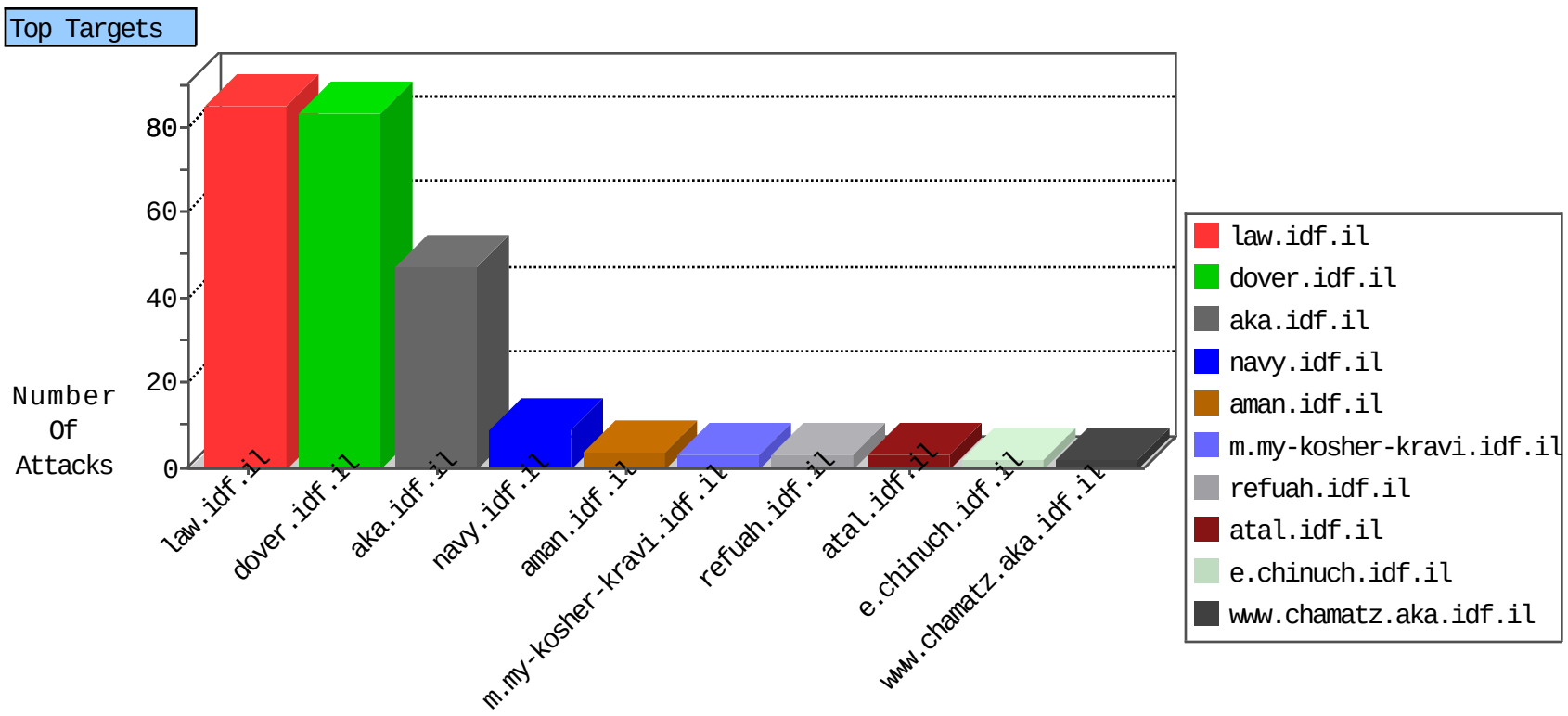
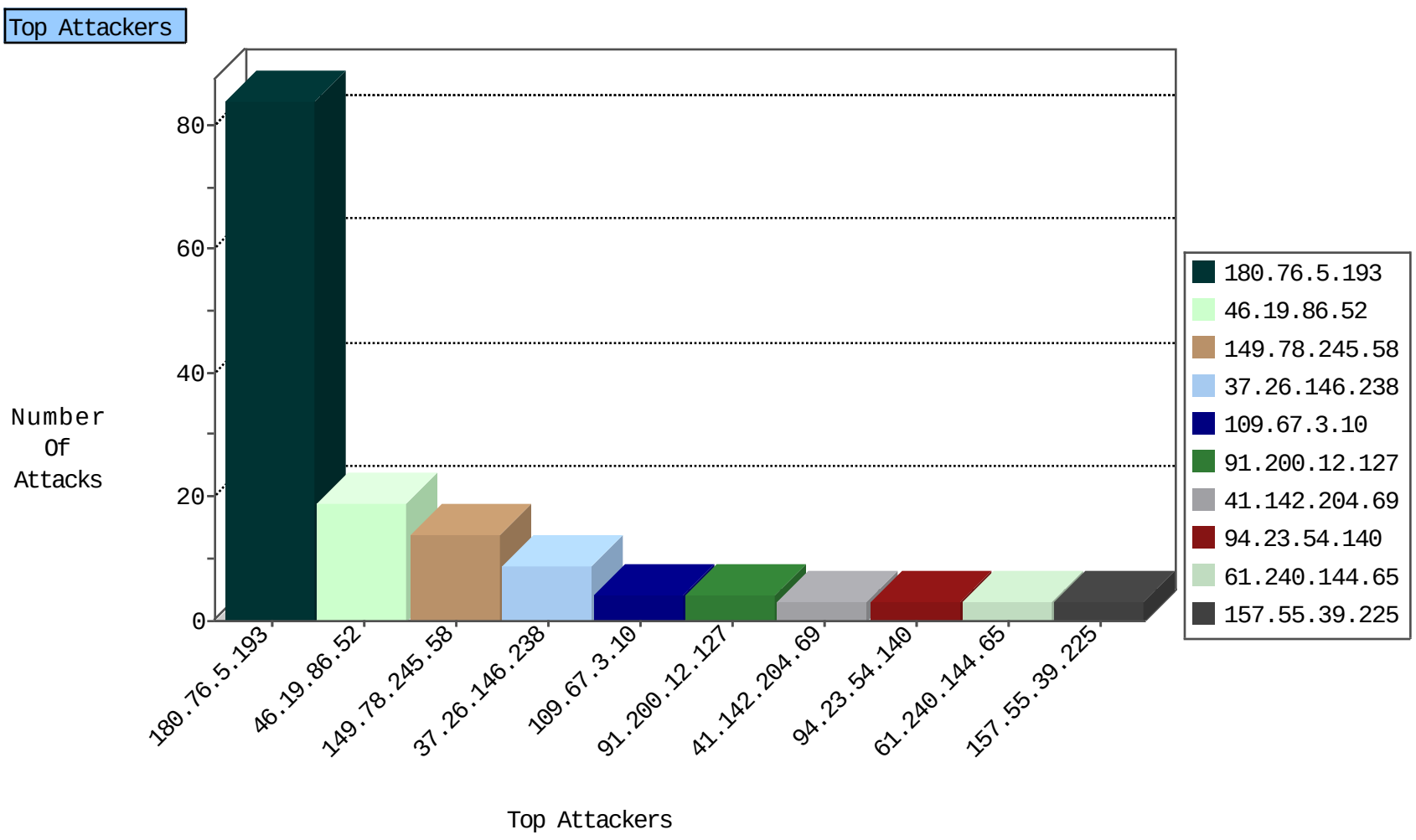
04-25-2015-17:03:09 to 04-25-2015-18:03:09

IDF Under Attack
04-25-2015-17:03:09

Top Targets



Top Attackers



04-25-2015-17:03:09 to 04-25-2015-18:03:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.69.42	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3

04-25-2015-17:03:09 to 04-25-2015-18:03:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.77.74	law.idf.il	DVRep_P-N_40-59	Permit	84
85.10.202.245	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	2
85.65.73.156	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	1
49.207.187.229	India	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
198.20.69.98	United States	147.237.8.27	e.madim.atal.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1

04-25-2015-17:03:09 to 04-25-2015-18:03:09

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	2
61.240.144.65	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.23.54.140	France	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
79.180.143.27	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
61.240.144.65	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
61.160.224.130	China	147.237.77.235	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1

04-25-2015-17:03:09 to 04-25-2015-18:03:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.86.52	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	19
149.78.245.58	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	14
109.67.3.10	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	4
79.181.120.54	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
66.249.73.193	United States	147.237.77.216	dover.idf.i	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
212.179.21.195	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
31.168.233.150	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
46.19.86.51	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	2
116.202.172.57	India	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
84.109.194.161	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
77.127.90.55	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
212.199.143.202	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
87.69.202.8	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
149.88.35.17	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
79.177.153.110	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
220.181.108.97	China	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
94.159.164.77	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	1
149.88.131.205	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
79.178.184.84	Israel	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
50.87.144.145	United States	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1
188.138.17.15	France	147.237.77.216	dover.idf.i	First packet isn't SYN	drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
37.26.146.238	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	9
79.177.164.105	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.121.142.186	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
91.200.12.127	Ukraine	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
91.200.12.127	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
84.94.19.38	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
157.55.39.8	United States	147.237.72.166	aka.idf.il	Unknown Parameter catId in www.aka.idf.il/tizmoret/	None	1
77.127.114.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/giyus/authenticationservice.asmx/getuserdetails	Block	1
66.249.75.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.173.171.236	Turkey	147.237.77.74	law.idf.il	Illegal HTTP Version	Block	1
41.142.204.69	Morocco	147.237.77.216	dover.idf.il	Malformed URL www.acunetix.wvs:443	Block	1
217.132.93.218	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
89.138.209.135	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.180.22.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
157.55.39.210	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/captcha.ashx	Block	1
66.249.79.106	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
93.173.143.88	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
46.121.77.247	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
180.76.6.144	China	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
85.65.193.69	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	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
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
107.178.195.193	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/tizmoret/news/mailto:	Block	1
41.142.204.69	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/jmx-console/htmladaptor	Block	1
91.200.12.22	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11845-en/dover.aspx/trackback/	Block	1
79.181.6.241	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
157.55.39.225	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il//captcha.ashx	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.79.114	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
94.23.54.140	France	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
188.165.15.13	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/russian/0502.stm	Block	1
85.250.48.184	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/authenticationservice.asmx/getuserdetails	Block	1
157.55.39.81	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/70344.jpg	Block	1
79.178.115.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/schar	Block	1
66.249.78.31	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/templatecontrols/generic/	Block	1
109.163.234.5	Romania	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
41.142.204.69	Morocco	147.237.77.216	dover.idf.il	WEB MISC Unauthorized File Access	None	1
79.182.32.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.225	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 157.55.39.225	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/klali/null	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/032204-1.stm	Block	1
94.23.54.140	France	147.237.77.216	dover.idf.il	Multiple signatures from 94.23.54.140	Block	1
54.204.243.45	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/iaf/present4.stm	Block	1
37.26.148.198	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/hebrew/ie-welcome.stm	Block	1
190.213.250.121	Trinidad and Tobago	147.237.72.156	aman.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
87.68.250.88	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42//894-he/refuah.aspx	Block	1
157.55.39.89	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1