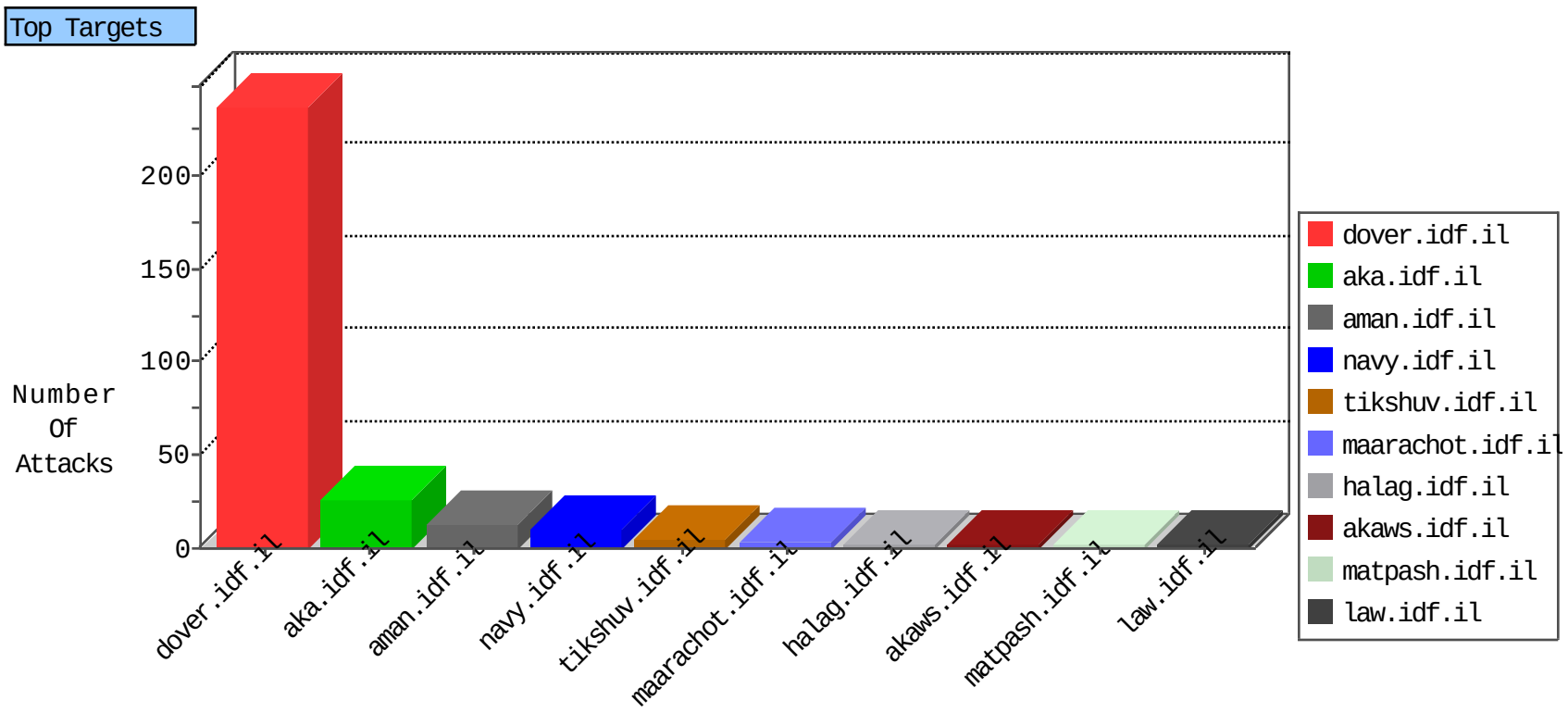
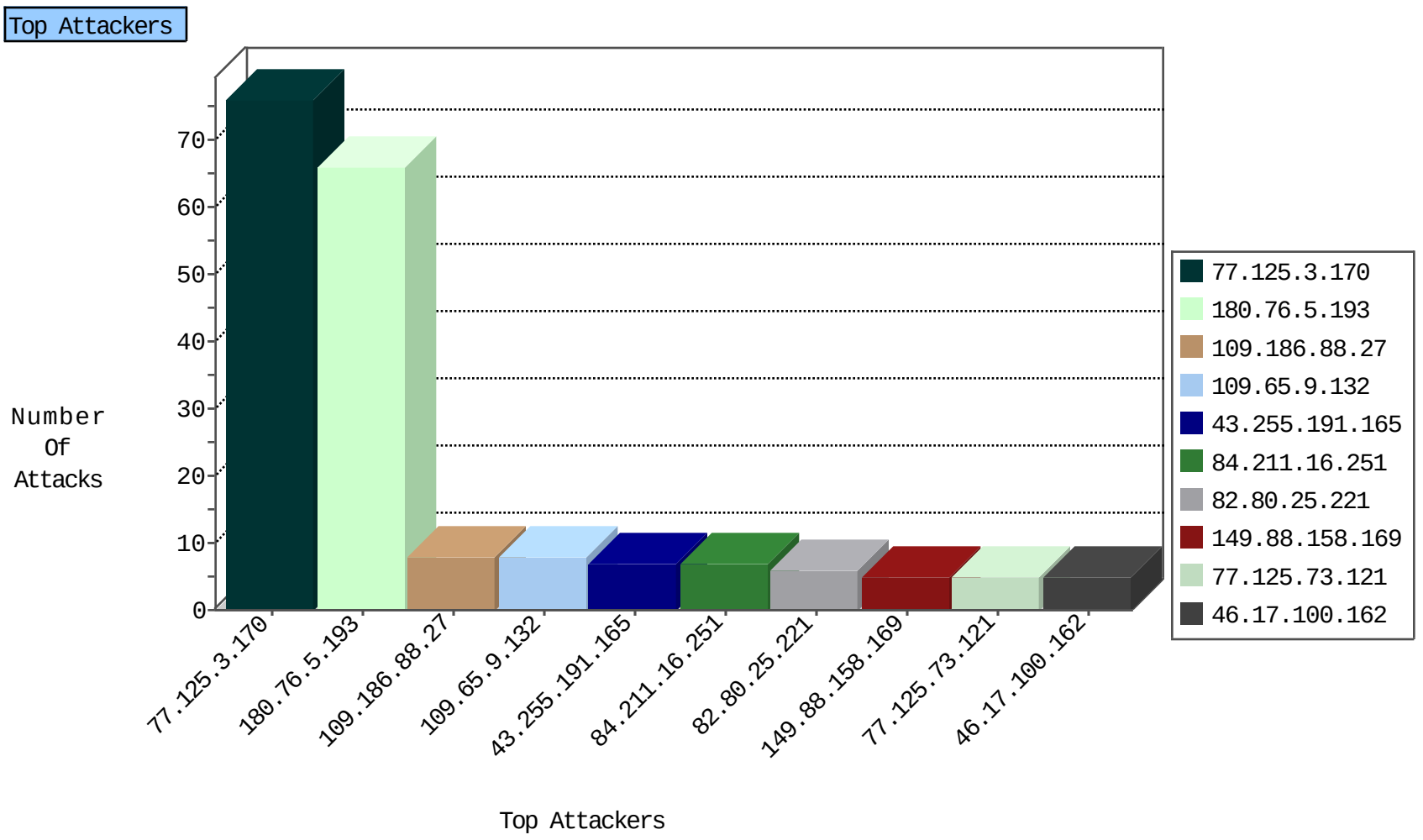
04-25-2015-12:03:05 to 04-25-2015-13:03:05

IDF Under Attack
04-25-2015-12:03:05

Top Targets



Top Attackers



04-25-2015-12:03:05 to 04-25-2015-13:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.69.50	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	6143
85.64.234.186	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	416
66.249.73.201	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	355
109.65.9.132	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	62
36.238.50.87	Taiwan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
212.199.182.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
87.68.80.179	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.78.197	Israel	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1
77.125.135.66	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
146.148.59.42		147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-25-2015-12:03:05 to 04-25-2015-13:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	66
192.116.188.117	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
37.205.9.131	Slovakia	147.237.72.156	aman.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
85.25.43.94	Germany	147.237.77.179	e.mazi.idf.il	DVRep_B-N_60_100	Block	1

04-25-2015-12:03:05 to 04-25-2015-13:03:05

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	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
87.69.227.40	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
46.17.100.162	Russian Federation	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
46.17.100.162	Russian Federation	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
163.32.234.3	Taiwan	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.8.46	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
61.240.144.67	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
46.17.100.162	Russian Federation	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
46.17.100.162	Russian Federation	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	Cote D'Ivoire	147.237.77.234	halag.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.165	Japan	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
163.32.234.3	Taiwan	147.237.72.217	e.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
79.178.145.177	Israel	147.237.0.34	tikshuv.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
61.160.224.130	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
46.17.100.162	Russian Federation	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1

04-25-2015-12:03:05 to 04-25-2015-13:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
77.125.3.170	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	76
109.186.88.27	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
84.211.16.251	Norway	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
129.100.205.213	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
84.108.87.99	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.65.209.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
207.46.13.95	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
149.88.158.169	United States	147.237.77.170	maarachot.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	2
46.19.86.196	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
149.88.158.169	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.66.147.164	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
89.139.48.0	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.201.194.12	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
77.125.73.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
93.215.75.193	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.153	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
198.58.102.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
108.59.253.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
84.191.87.162	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
37.26.147.184	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
174.1.109.114	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
198.20.69.74	United States	147.237.76.148	gqcenter.aka.idf.il		drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
89.138.67.196	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	5
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	4
84.108.211.12	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	3
77.125.73.121	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	3
93.172.169.104	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	3
77.127.182.86	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
66.249.69.99	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/shared/ajax/setivgallerycontrol.aspx	Block	2
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	2
157.55.39.59	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/pakar13.stm	Block	1
66.249.75.74	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/994-8775-he/navy.aspx	Block	1
194.187.168.19	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/idf_in_pictures/2000/october/piguim.stm	Block	1
66.249.69.83	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il//shared/ajax/setivgallerycontrol.aspx	Block	1
109.186.22.78	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
213.57.237.48	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.166	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
85.65.15.253	Israel	147.237.72.166	aka.idf.il	Unknown Parameter _ in www.aka.idf.il/main/home/default.aspx	None	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1400-he/atal.aspx	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Malformed URL	Block	1
66.249.69.92	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
149.88.158.169	United States	147.237.77.170	maarachot.idf.il	CVE-2011-3192:Apache_httpd_Remote_Denial_of_Service_ME	Block	1
79.178.107.241	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal/mavo-natziv2001.stm	Block	1
85.250.105.118	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Multiple Malformed URL from 202.112.50.77	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.181.140.155	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/faq.aspx	None	1
14.153.132.131	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 202.112.50.77	Block	1
157.55.39.59	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.59	Block	1
83.49.122.137	Spain	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/english/	Block	1
66.249.75.62	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
180.76.4.112	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
46.117.206.215	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
77.126.118.225	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
202.112.50.77	China	147.237.77.216	dover.idf.il	Unknown HTTP Request Method quit in URL	Block	1