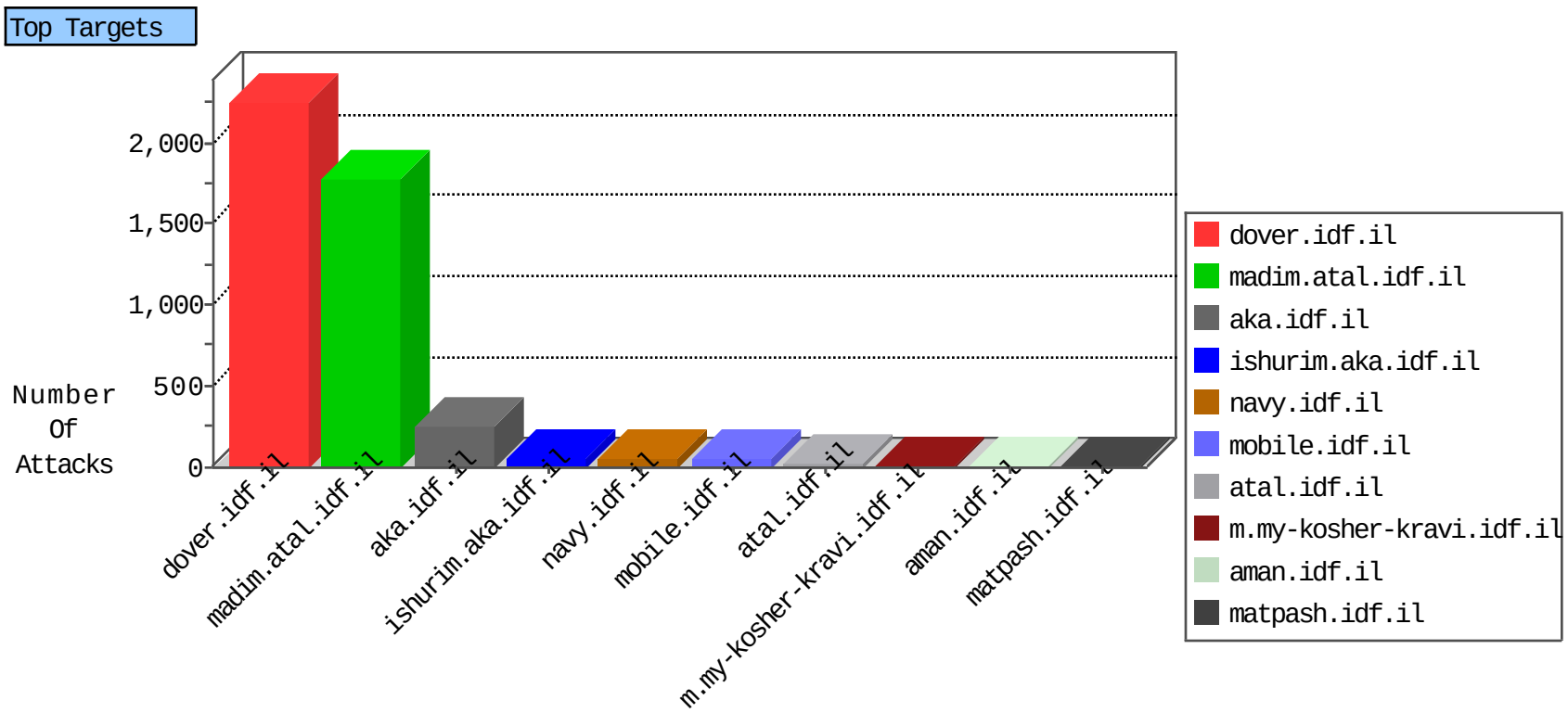
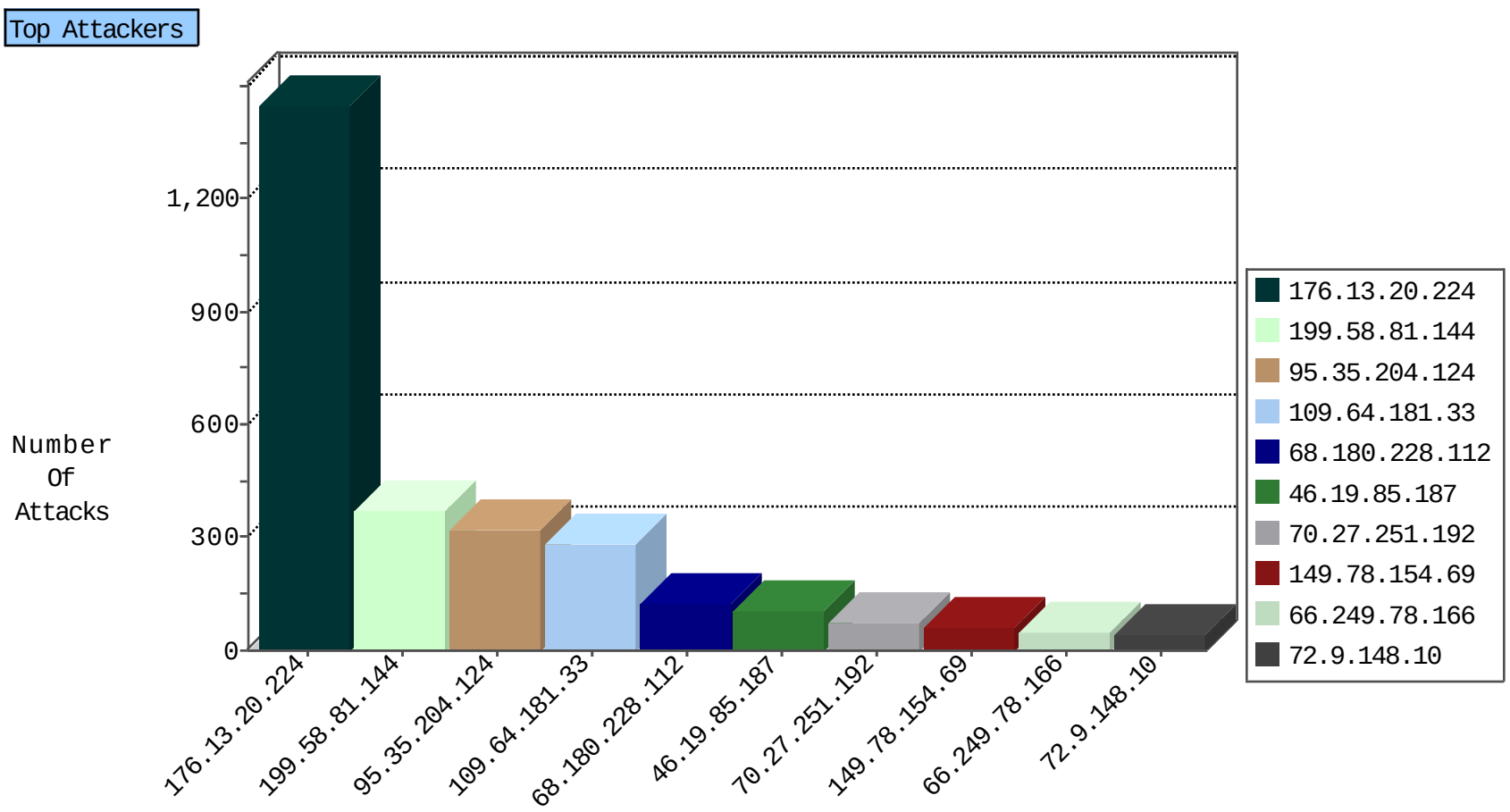
10-27-2015-07:05:58 to 10-27-2015-08:05:58

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-27-2015-07:05:58 to 10-27-2015-08:05:58

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.150.20	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	321
199.58.81.144	Canada	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	255
62.90.139.75	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
109.65.17.219	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	18
176.13.16.219	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.179.140.240	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	6
62.90.139.75	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
70.199.71.63	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
109.67.35.144	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.228.142.125	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
186.29.108.93	Colombia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
45.63.1.137		147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
79.178.33.166	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
186.29.108.93	Colombia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
176.12.146.64	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
176.13.20.224	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
176.12.146.64	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.6.98	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-27-2015-07:05:58 to 10-27-2015-08:05:58

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.81.144	Canada	147.237.77.216	dover.idf.il	10725: TCP: LOIC DDoS Tool	Block	5

10-27-2015-07:05:58 to 10-27-2015-08:05:58

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

10-27-2015-07:05:58 to 10-27-2015-08:05:58

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.64.181.33	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	284
199.58.81.144	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	150
46.19.85.187	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	102
70.27.251.192	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	74
199.58.81.144	Canada	147.237.77.216	dover.idf.i	drop		drop	52
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
199.58.81.144	Canada	147.237.77.216	dover.idf.i	drop	SAM rule	drop	44
46.19.86.202	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	41
212.179.21.194	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
77.126.1.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
109.195.95.90	Russian Federation	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
66.249.78.166	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
79.182.164.20	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
77.125.151.221	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
64.233.172.155	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
70.199.71.63	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
109.67.35.144	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
176.13.9.70	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	22
66.249.78.159	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
2.52.36.13	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
100.100.54.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19
64.233.172.171	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
154.118.241.30		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	15
79.179.140.240	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
64.233.172.163	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
93.172.132.177	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
208.69.40.101	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
75.82.50.94	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
100.100.42.236		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
62.90.139.75	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
176.13.9.37	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
31.168.197.78	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
186.29.108.93	Colombia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
37.26.146.197	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
207.46.13.144	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
40.77.167.35	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
80.246.133.198	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
157.55.39.221	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
40.77.167.39	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
194.90.241.111	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
84.111.138.75	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.20.224	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.20.224	Block	1421
95.35.204.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	308
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 68.180.228.112	Block	70
188.120.159.92	Israel	147.237.72.167	ishurim.aka.idf.il	PHP Attempt	Block	42
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	42
176.13.20.224	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	20
68.180.228.112	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /mivtza>×¡×Ÿ×•×¦×˜×›×Ã¼×?×ž×œ ×¡×?×™×¢×•, ×¡×ž×—×″×?×?×?×ž×œ ×″×›Ã¿ â€Ž×¢×˜×¥ ×¦×•×›×•×™. <table cellspacing=	Block	14
46.19.86.33	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
207.46.13.35	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/miluimday.asp	Block	14
84.229.208.222	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
66.249.64.244	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	14
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/16946.jpg	Block	14
175.44.4.119	China	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/eitan/main/	Block	14
207.46.13.35	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/eitan/listpage/default.asp	None	14
54.209.60.63	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
188.165.234.68	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.234.68	Block	14
87.69.87.39	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Double URL Encoding - parameter: ReturnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
199.16.156.125	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/6/size220x0/17436.jpg	Block	14
176.12.137.113	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	14
207.46.13.35	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/chinuch/faq/default.asp	None	14
66.249.64.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
188.165.234.68	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
199.59.148.211	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/6/size220x0/17436.jpg	Block	14
216.218.206.66	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	14
66.249.64.178	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
194.90.241.111	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
95.35.204.124	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
46.19.85.51	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
199.168.141.174	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-15916-en/dover.aspx/trackback/	Block	14
79.181.112.133	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	14
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
199.16.156.124	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/6/size220x0/17436.jpg	Block	14
157.55.39.127	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	14