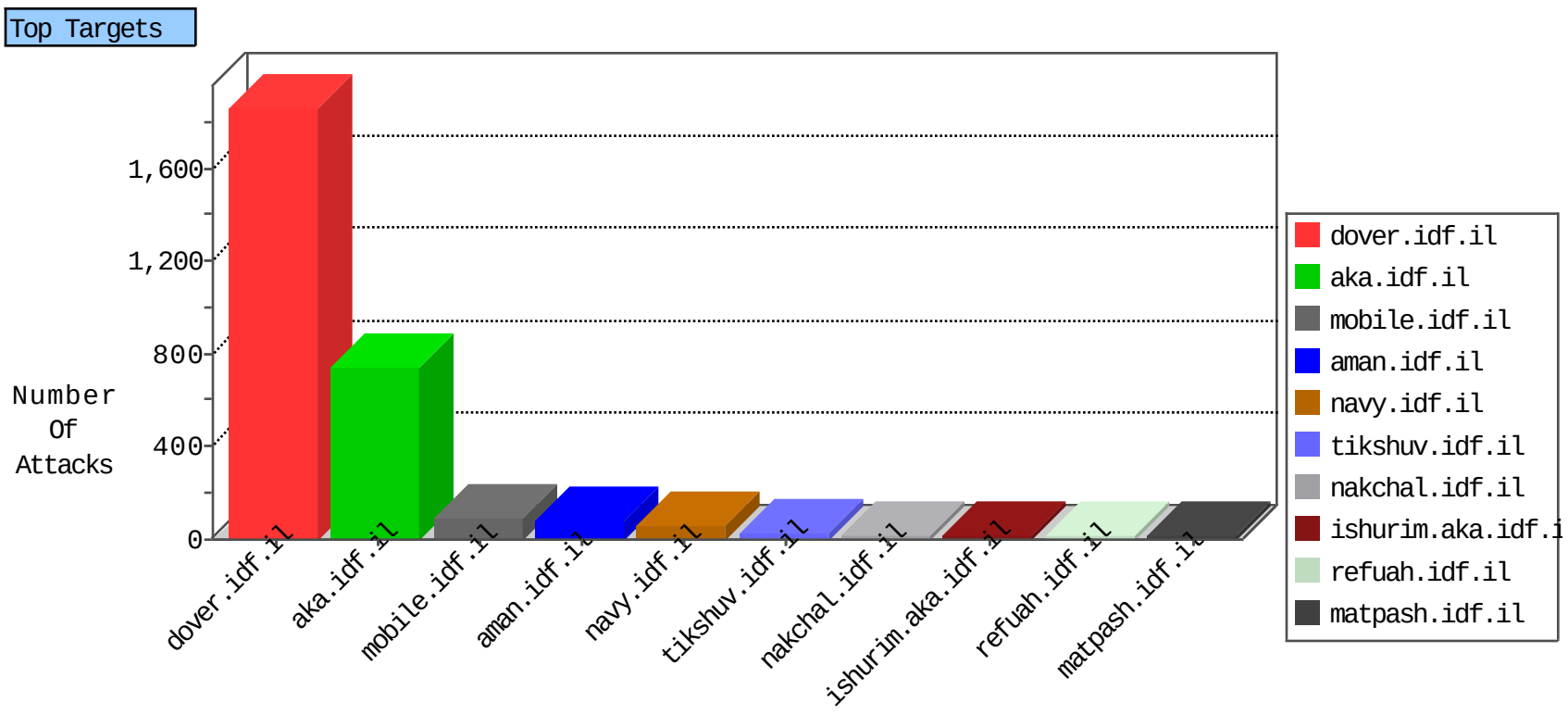
10-23-2015-02:04:05 to 10-23-2015-03:04:05

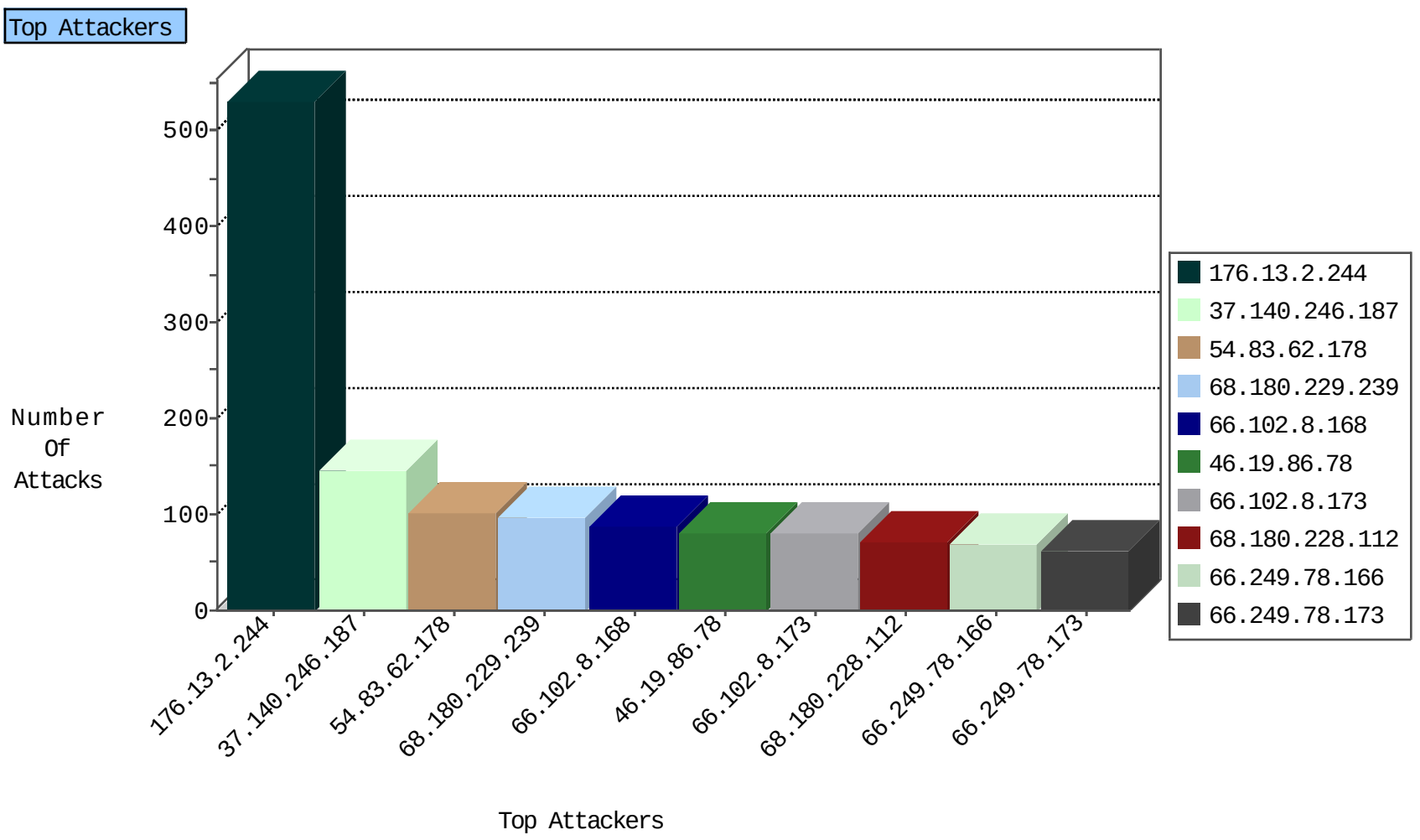
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-23-2015-02:04:05 to 10-23-2015-03:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
75.136.218.159	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	53
79.183.160.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	21
31.154.190.5	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	16
46.19.85.146	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
37.75.213.133	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
2.54.162.234	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
104.193.10.60	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

10-23-2015-02:04:05 to 10-23-2015-03:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-23-2015-02:04:05 to 10-23-2015-03:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
223.4.174.30	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
223.4.174.30	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.107.17.72	147.237.0.19	Seychelles	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
188.18.51.39	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
188.18.51.39	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN Potential SSH Scan	1
123.151.149.222	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
5.11.41.55	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
223.4.174.30	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
188.18.51.39	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN Potential SSH Scan	1
188.18.51.39	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
188.18.51.39	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

10-23-2015-02:04:05 to 10-23-2015-03:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.140.246.187	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	130
54.83.62.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	102
46.19.86.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	81
66.102.8.168	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	64
71.200.16.138	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
212.143.40.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
5.109.100.188	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
185.120.126.13		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
66.102.8.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
2.54.11.179	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
46.19.86.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
46.19.86.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
66.102.8.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.102.8.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
66.102.8.178	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.85.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
87.142.126.35	Germany	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	20
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
66.249.84.167	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.84.165	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
207.118.94.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
199.16.156.125	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
194.90.209.198	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
199.16.156.124	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
217.227.27.20	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.177.98.71	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
199.16.156.126	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
84.111.197.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
139.162.207.73	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
109.65.21.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
68.180.229.239	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
37.236.136.16	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
75.136.218.159	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
71.34.72.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9

10-23-2015-02:04:05 to 10-23-2015-03:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.2.244	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 176.13.2.244	Block	532
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	84
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	56
176.12.138.97	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	42
198.105.221.6	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 198.105.221.6	Block	28
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
217.227.27.20	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	14
37.140.246.187	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	14
182.118.60.176	China	147.237.0.34	tikshuv.idf.il	URL is Above Root Directory www.tikshuv.idf.il/../shared/clientscripts/jquery.plugins/slider.js	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	14
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/17396.jpg	Block	14
157.55.39.255	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
46.19.85.171	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	14
66.249.75.7	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/	Block	14
202.46.52.165	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	14
66.249.65.51	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/sachar/klali.aspx	Block	14
198.105.221.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	14
141.212.122.96	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /x	Block	14
66.249.75.23	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/	Block	14
207.46.13.119	United States	147.237.72.166	aka.idf.il	Unknown Parameter sig2 in www.aka.idf.il/main/giyus/general.aspx	None	14
2.54.11.179	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	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/4/size220x0/17374.jpg	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	14
217.227.27.20	Germany	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 217.227.27.20	Block	14
17.138.60.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	14
180.76.15.139	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/	Block	14
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	14
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/4/size220x0/17404.jpg	Block	14
157.55.39.11	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/_incapsula_resource	Block	14

10-23-2015-02:04:05 to 10-23-2015-03:04:05