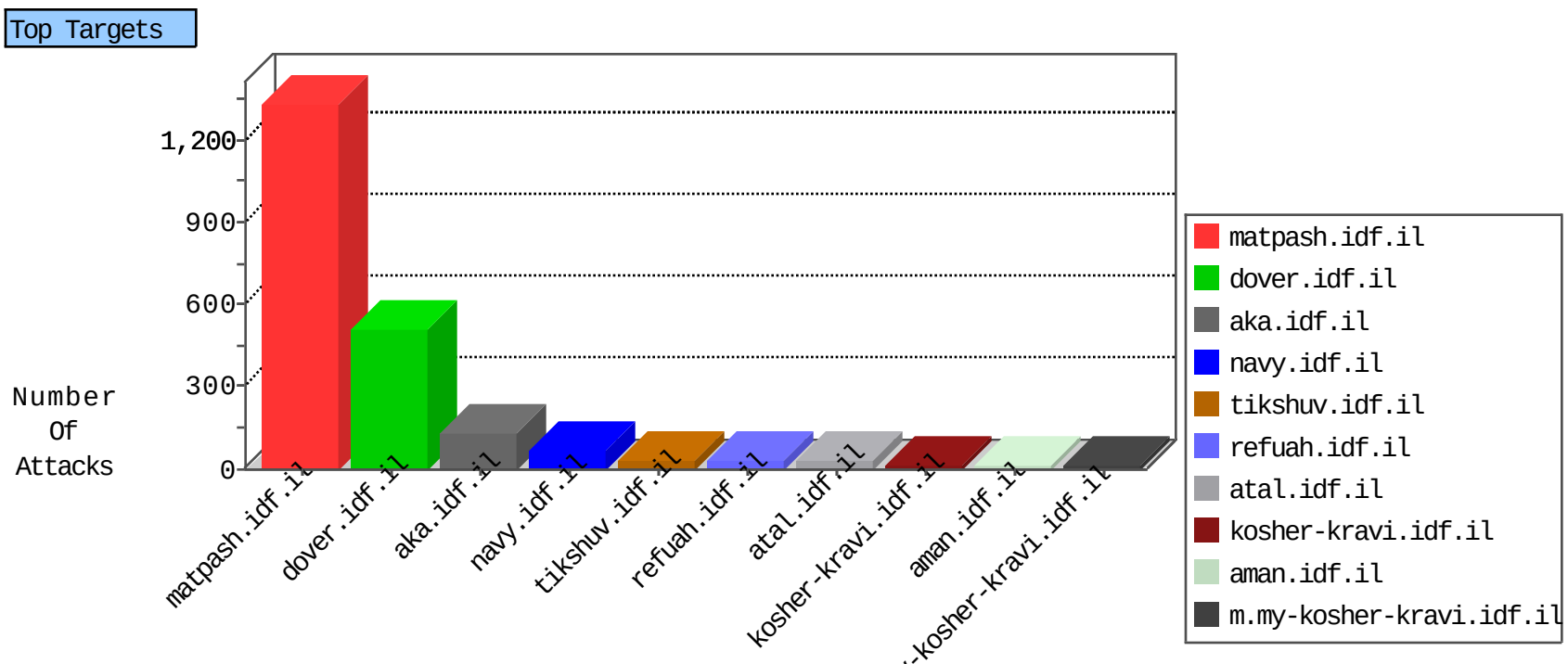
10-24-2015-06:04:09 to 10-24-2015-07:04:09

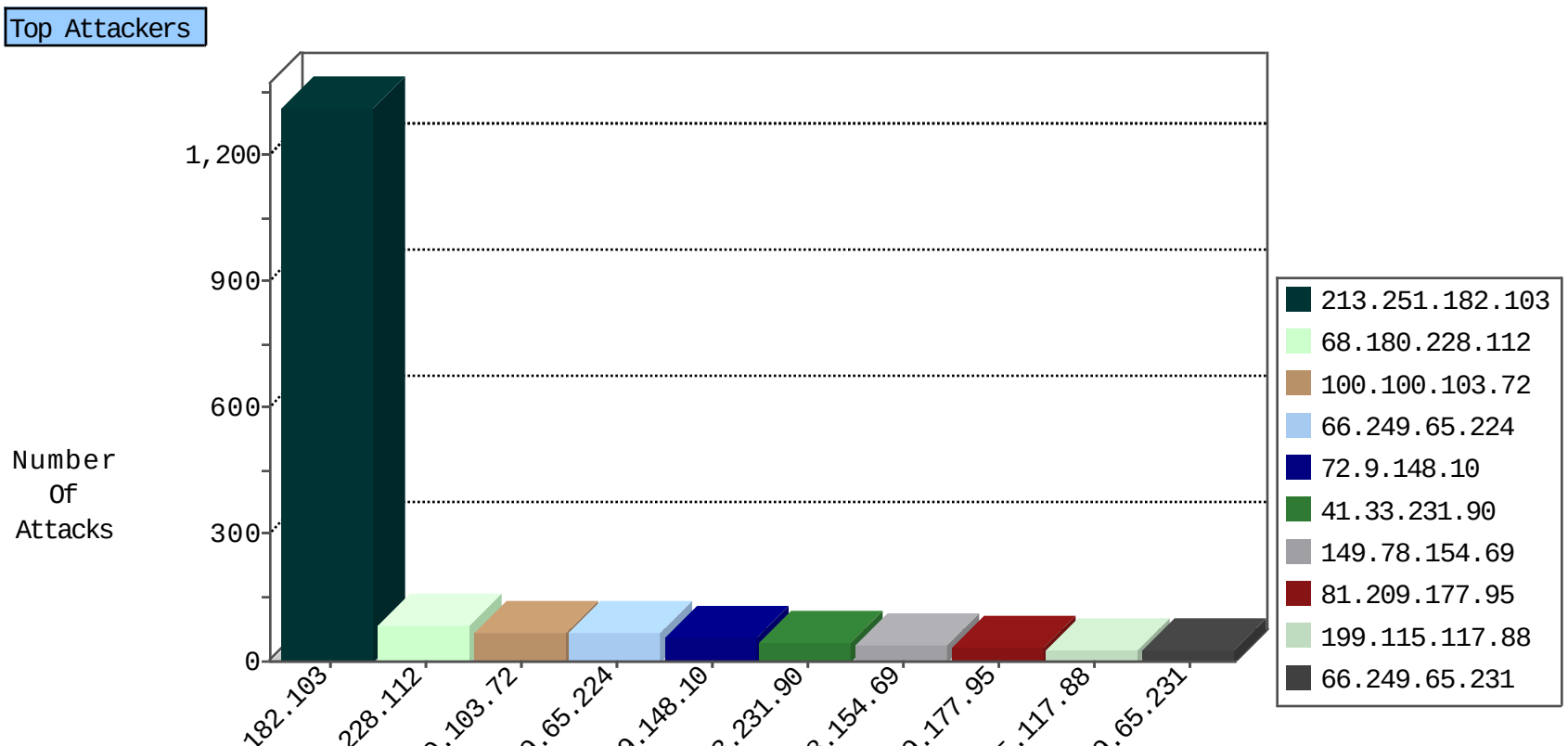
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-24-2015-06:04:09 to 10-24-2015-07:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.59.117.15	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
222.186.56.115	China	147.237.0.15	kosher-kravi.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
222.186.56.115	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
188.138.1.218	Germany	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

10-24-2015-06:04:09 to 10-24-2015-07:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-24-2015-06:04:09 to 10-24-2015-07:04:09

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	2
93.174.89.142	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
101.183.79.112	147.237.77.216	Australia	dover.idf.il	portscan: TCP Distributed Portscan	1

10-24-2015-06:04:09 to 10-24-2015-07:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
100.100.103.72		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	57
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
17.142.156.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
100.100.103.72		147.237.0.19	madim.atal.idf.i	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
119.15.2.10	New Zealand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
78.53.233.229	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
174.95.94.22	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
78.53.233.229	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
8.37.228.81	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.65.224	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.67.34	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.132.109	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
41.232.124.217	Egypt	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3
37.142.108.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
40.77.167.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.67.27	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
8.37.228.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	3
207.46.13.186	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
8.37.227.70	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
70.39.186.222	Satellite Provid	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
177.188.116.189	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
87.69.44.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.52.137.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
198.58.99.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
108.36.255.214	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
8.37.227.70	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
198.58.102.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
72.192.201.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
188.165.15.126	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
133.130.58.190	Japan	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
81.209.177.95	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2

10-24-2015-06:04:09 to 10-24-2015-07:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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	1315
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	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
144.76.44.148	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	14
188.165.15.162	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9686-he/refuah.aspx	Block	14
91.191.151.99	France	147.237.72.166	aka.idf.il	PHP Attempt	Block	14
54.179.134.216	Singapore	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	14
172.102.192.188		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/english/rk=0/rs=0ynkw88ll5r75x26kow.1lrd0_y-	Block	14
198.52.212.37	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/english/rk=0/rs=0ynkw88ll5r75x26kow.1lrd0_y-	Block	14
91.191.151.99	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-admin/setup-config.php	Block	14
66.249.64.244	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
180.76.15.136	China	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
81.209.177.95	Europe	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	14
199.115.117.88	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/themes/elastixneo/ie.css	Block	14
112.253.25.53	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	14
66.249.65.241	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/894-he	Block	14
182.118.71.25	China	147.237.76.86	navy.idf.il	URL is Above Root Directory www.navy.idf.il/../shared/clientscripts/jquery.plugins/slider.js	Block	14
81.209.177.95	Europe	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	14
5.175.25.171	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	14
199.115.117.88	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/themes/elastixneo/ie.css	Block	14
141.212.122.160	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	14
66.249.78.94	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	14
188.165.15.37	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1406-he/atal.aspx	Block	14
45.57.139.21		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/rk=0/rs=0ynkw88ll5r75x26kow.1lrd0_y-	Block	14
81.209.177.189	Europe	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	12

10-24-2015-06:04:09 to 10-24-2015-07:04:09