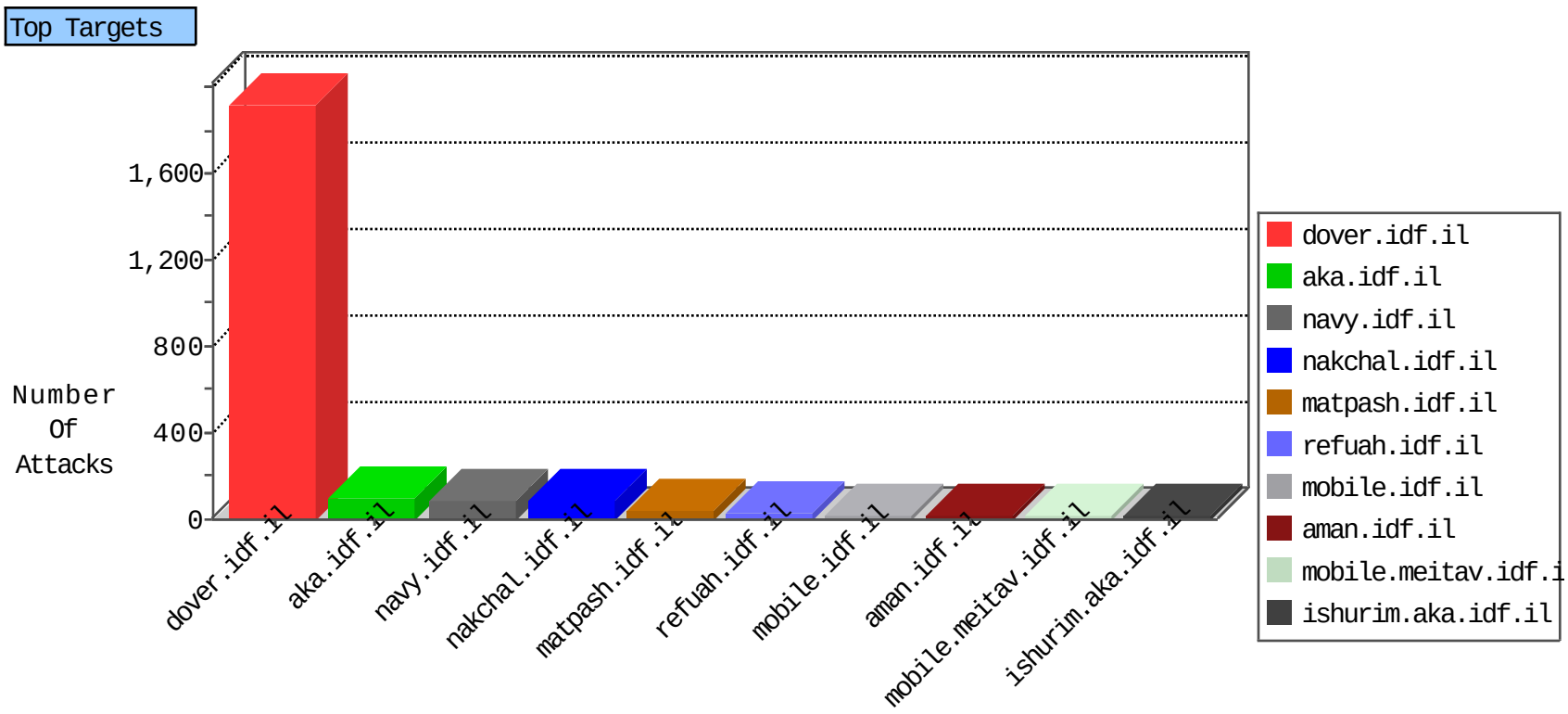
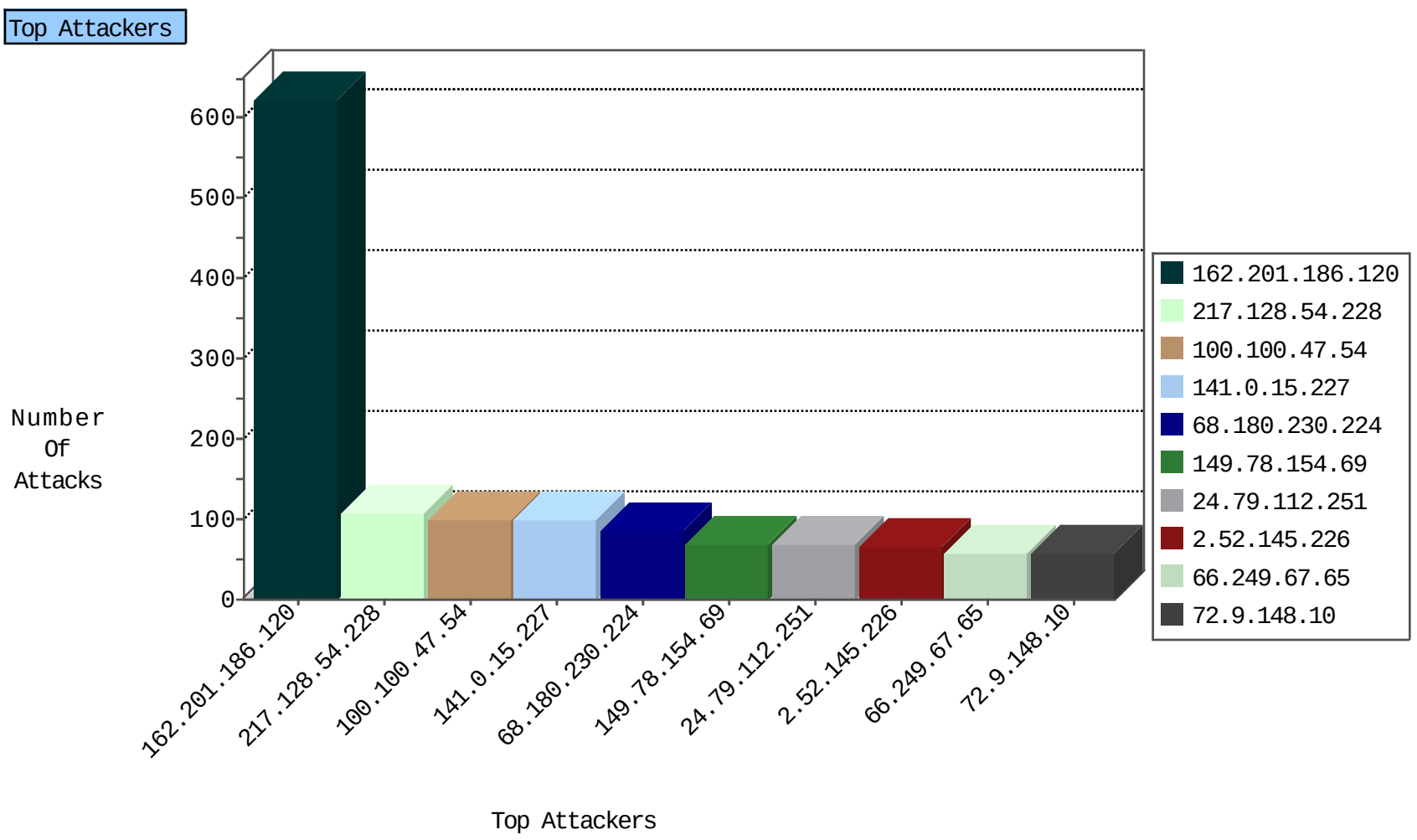
10-25-2015-02:04:01 to 10-25-2015-03:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-25-2015-02:04:01 to 10-25-2015-03:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.114.188	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	10

10-25-2015-02:04:01 to 10-25-2015-03:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-25-2015-02:04:01 to 10-25-2015-03:04:01

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	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
87.126.111.74	147.237.0.33	Bulgaria	idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
46.151.52.8	147.237.8.45	Ukraine	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
128.199.236.67	147.237.0.19	Singapore	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
117.135.163.104	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -f -sS	1
54.215.188.240	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
117.135.163.104	147.237.0.35	China	akaws.idf.il	ET SCAN NMAP -sS window 2048	1

10-25-2015-02:04:01 to 10-25-2015-03:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
162.201.186.120	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	624
217.128.54.228	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	106
141.0.15.227	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	98
24.79.112.251	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	69
2.52.145.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	66
85.250.52.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
2.54.34.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
68.180.230.29	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	34
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	25
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
100.100.47.54		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
24.189.121.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
100.100.47.54		147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	16
100.100.47.54		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
100.100.47.54		147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	14
100.100.47.54		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.179.183.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.69.160.29	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.237.204.65	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.96.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.99.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.29.153.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
86.161.3.59	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
37.142.108.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.178.206.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
100.100.47.54		147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	9
64.233.172.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.52.38.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.142.108.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
72.239.89.93	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
100.100.47.54		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.179.205.211	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
219.74.36.138	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.221.242	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.132.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.57.165.6	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
87.93.159.241	Finland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

10-25-2015-02:04:01 to 10-25-2015-03:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1111-he/nakhal.aspx	Block	84
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	56
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/bagatz_sarbanim.stm_	Block	28
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
84.108.129.6	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/news/	Block	14
66.249.69.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
64.19.78.242	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	14
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	14
146.185.234.48	Russian Federation	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/links/links.aspx/templates/sendtofriend/sendtofriend.aspx	Block	14
66.249.69.18	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	14
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
74.82.47.3	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	14
66.249.67.77	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/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_pictures.asp	Block	14
81.177.166.161	Russian Federation	147.237.77.216	dover.idf.il	Admin Blocking	Block	14
66.249.67.83	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	14
2.54.30.144	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	14
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	14
81.177.166.161	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin	Block	14
66.249.67.89	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	14
46.4.94.226	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/robots.txt	Block	14
199.127.226.150	United States	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	12

10-25-2015-02:04:01 to 10-25-2015-03:04:01