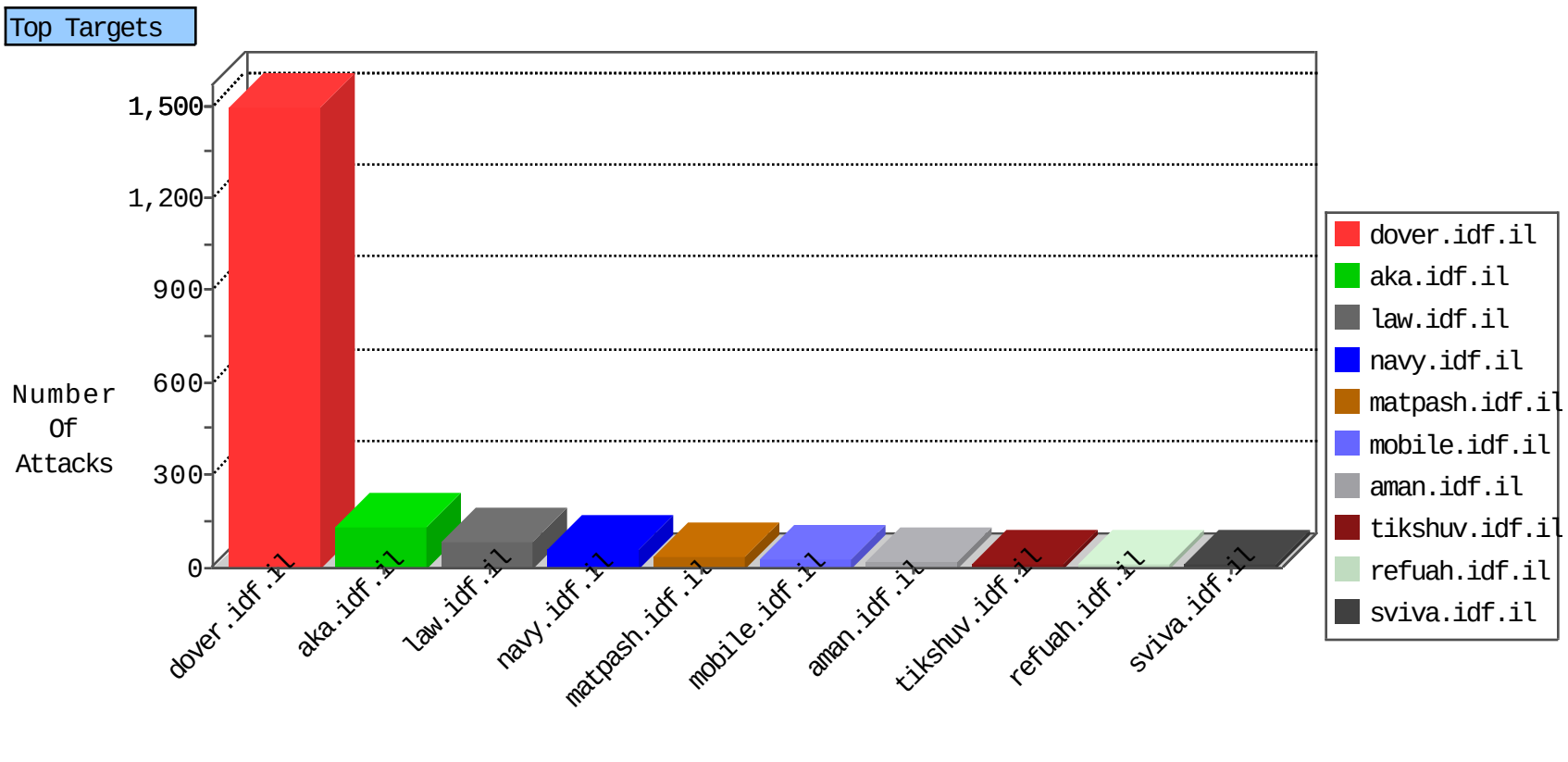
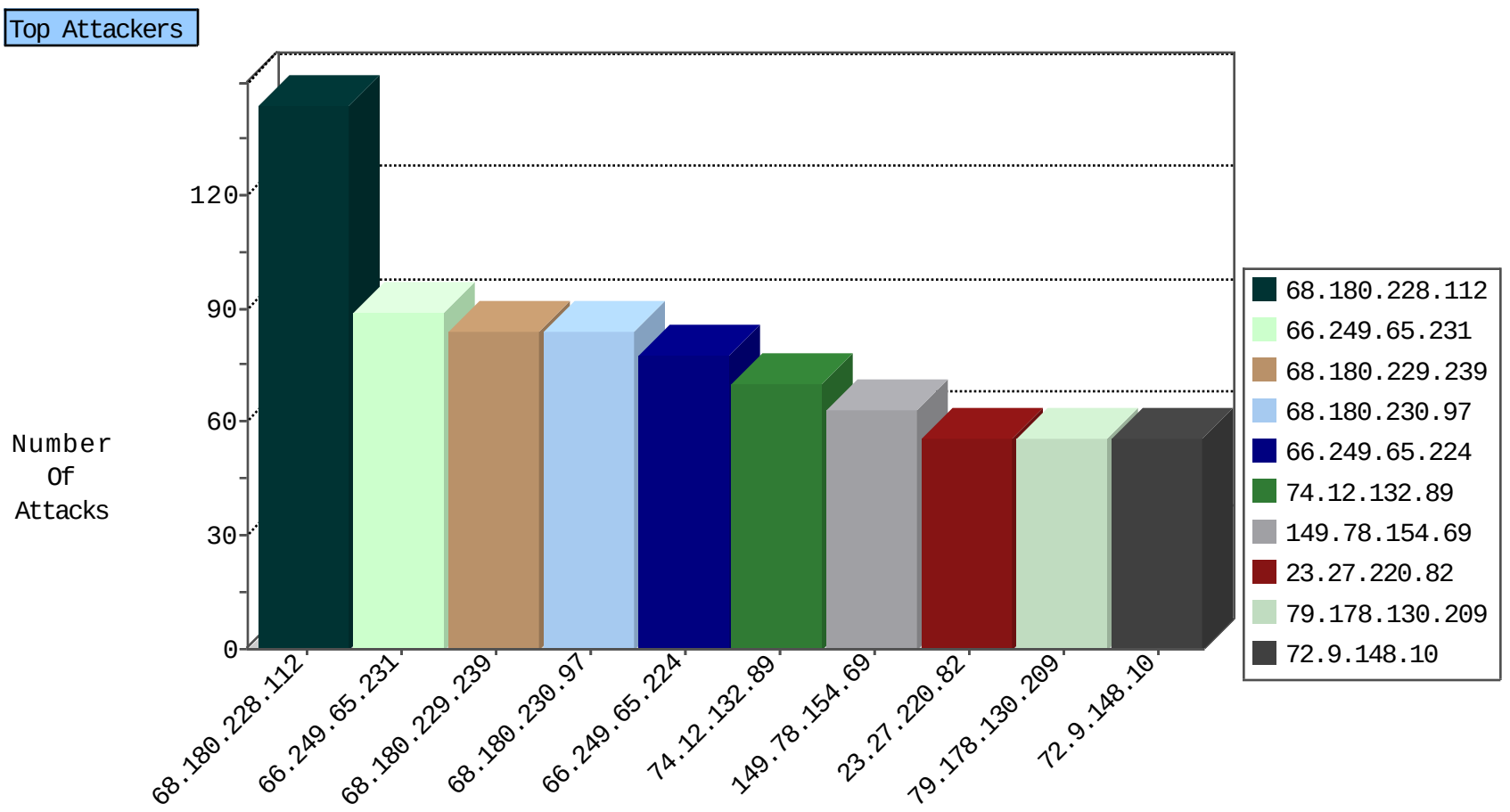
10-24-2015-01:04:09 to 10-24-2015-02:04:09

IDF Under Attack Daily Report





10-24-2015-01:04:09 to 10-24-2015-02:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
88.238.81.103	Turkey	147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
66.249.93.238	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
2.54.156.187	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
92.241.42.63	Jordan	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
79.182.142.7	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
134.147.203.115	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2
79.182.142.7	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
38.70.6.32	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
45.32.68.116		147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

10-24-2015-01:04:09 to 10-24-2015-02:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.237.232.46	Iraq	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	4

10-24-2015-01:04:09 to 10-24-2015-02:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.234.17.46	147.237.77.216	Egypt	dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
93.174.93.138	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
81.192.139.152	147.237.76.147	Morocco	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
46.2.161.169	147.237.76.30	Turkey	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
93.174.93.138	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
78.30.208.199	147.237.77.243	Russian Federation	mobile.idf.il	ET SCAN NMAP -sS window 1024	1

10-24-2015-01:04:09 to 10-24-2015-02:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
74.12.132.89	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
23.27.220.82	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
79.178.130.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
5.29.82.45	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	45
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
23.27.248.205	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
2.54.156.187	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	34
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
72.160.215.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	25
76.189.105.19	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
67.148.50.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
88.238.81.103	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.87.19.109	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
40.77.167.37	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
40.77.167.35	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.149.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
37.237.232.118	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
92.241.42.63	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
72.28.218.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.237.232.138	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
87.68.34.95	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.237.232.138	Iraq	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.237.232.58	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.65.168.248	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.186.14.66	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.237.232.25	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.237.232.139	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.237.232.78	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.237.232.147	Iraq	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
78.53.226.50	Germany	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.142.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.21	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6

10-24-2015-01:04:09 to 10-24-2015-02:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.230.97	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	84
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/qeneral/default.a	Block	84
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	70
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	Distributed Suspicious Response Code	Block	56
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	28
46.60.38.8	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22777-ar/dover.aspx)	Block	28
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
144.76.23.202	Germany	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/1367-8729-he/	Block	14
66.249.65.234	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/894-he	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	14
157.55.39.237	United States	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	14
46.116.128.95	Israel	147.237.72.166	aka.idf.il	Unknown Parameter _ in www.aka.idf.il/main/giyus/userdetails/updateuserdetails.aspx	None	14
85.250.103.33	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	14
66.249.65.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	14
176.12.147.191	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/giyus	Block	14
54.179.134.216	Singapore	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to /	Block	14
93.173.176.204	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	14
220.181.108.101	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	14
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	14
141.212.122.160	United States	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/	Block	14
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	14

10-24-2015-01:04:09 to 10-24-2015-02:04:09