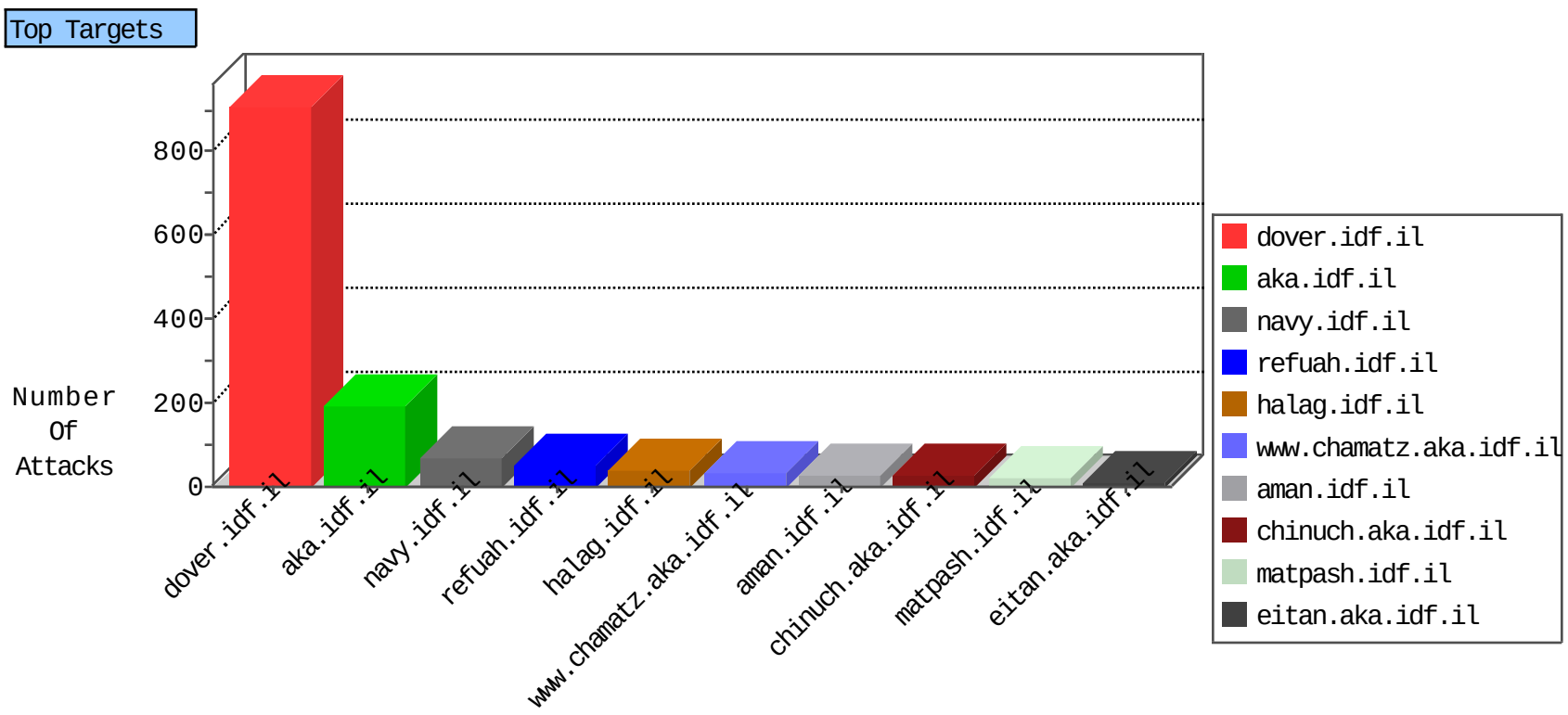
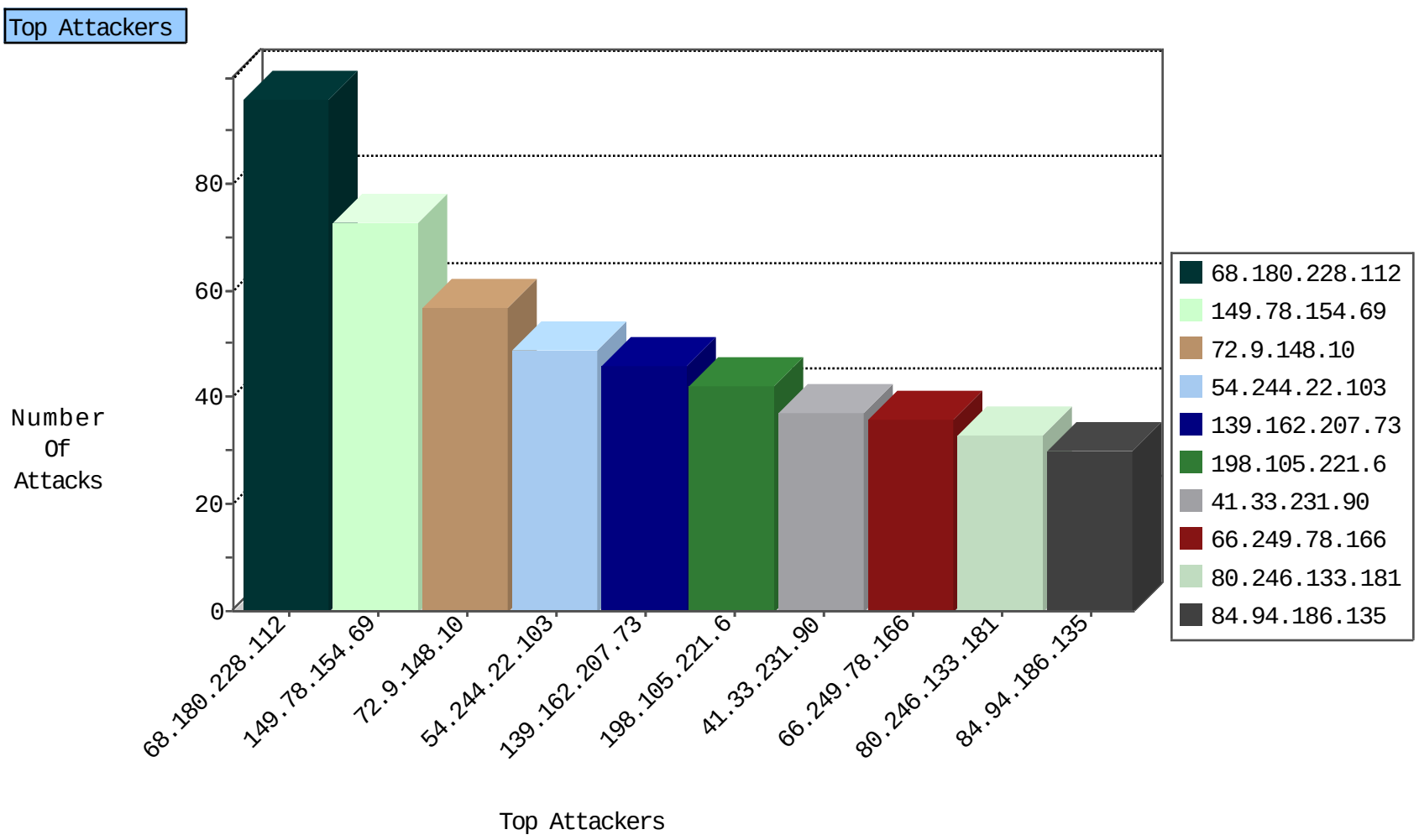
10-23-2015-03:04:08 to 10-23-2015-04:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-23-2015-03:04:08 to 10-23-2015-04:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
58.48.255.12	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
176.13.13.177	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
182.243.159.251	China	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

10-23-2015-03:04:08 to 10-23-2015-04:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-23-2015-03:04:08 to 10-23-2015-04:04:08

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
193.107.16.206	147.237.76.202	Russian Federation	e.halag.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
180.179.49.154	147.237.77.227	India	e.hamaz.idf.il	ET SCAN NMAP -sS window 2048	1
139.162.128.105	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential SSH Scan	1
58.253.96.122	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
209.41.67.92	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.16.206	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
180.179.49.154	147.237.77.227	India	e.hamaz.idf.il	ET SCAN NMAP -sS window 4096	1
180.179.49.154	147.237.77.227	India	e.hamaz.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.194	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
209.41.67.92	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1

10-23-2015-03:04:08 to 10-23-2015-04:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
139.162.207.73	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
54.244.22.103	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
84.94.186.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
80.246.133.181	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	29
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
66.249.84.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
70.70.53.205	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
77.125.153.179	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
66.102.8.178	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
221.121.150.199	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
207.46.13.178	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
209.122.120.59	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
40.77.167.3	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.102.8.168	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
70.162.28.25	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
221.121.151.182	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.88.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
134.191.232.71	Israel	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.180.138.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.142.102.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.88.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.102.8.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
125.215.235.181	Hong Kong	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.255	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.108.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
100.100.64.27		147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	6
203.127.96.204	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
66.102.8.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
40.77.167.3	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.102.8.173	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.84.165	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

10-23-2015-03:04:08 to 10-23-2015-04:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	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
198.105.221.6	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 198.105.221.6	Block	42
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_text.asp	Block	28
134.191.232.69	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	14
66.249.67.217	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	14
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1129-he/kkkkkkk=58dc99e5kkkkkkk_58dc99e5	Block	14
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	14
141.212.122.96	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /x	Block	14
66.249.75.15	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/	Block	14
185.10.107.68	Europe	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il/	Block	14
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	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
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.67.133	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
157.55.39.133	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/templates/shared/usercontrols/trajector/	Block	14
207.46.13.48	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	14
83.31.137.75	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/dover.aspx/	Block	14
66.249.67.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/mainpage	Block	14
176.28.46.163	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/qeneral/default.a	Block	14
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
38.111.147.88	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
207.46.13.119	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14

10-23-2015-03:04:08 to 10-23-2015-04:04:08