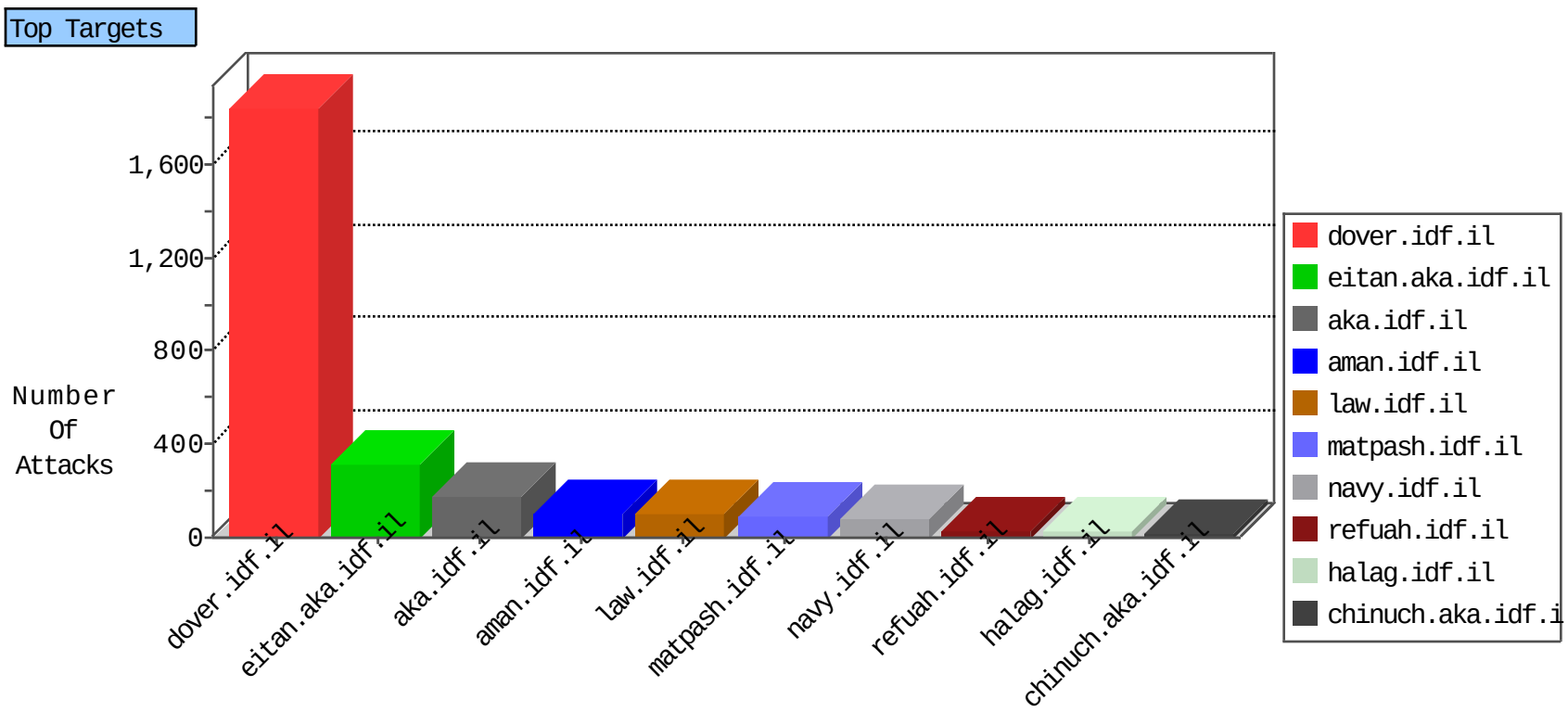
10-24-2015-00:04:08 to 10-24-2015-01:04:08

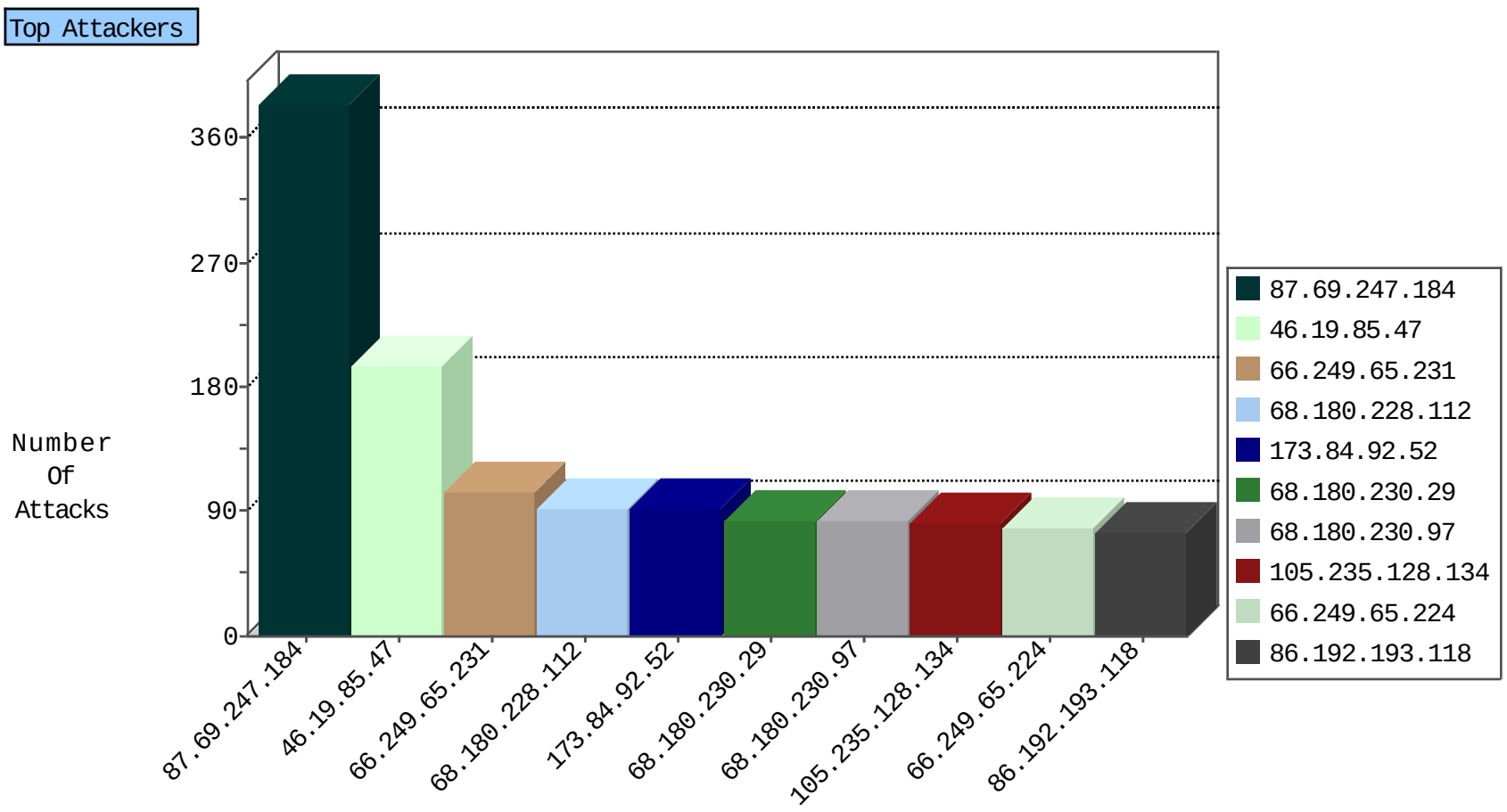
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-24-2015-00:04:08 to 10-24-2015-01:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.234.17.46	Egypt	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	345
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	31
108.45.80.52	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
93.173.15.200	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
213.57.90.158	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
185.23.124.72	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
45.32.68.116		147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
89.248.172.154	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
141.212.121.191	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
71.6.135.131	United States	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.154	Netherlands	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
2.54.191.59	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
89.248.172.154	Netherlands	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
89.248.172.154	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

10-24-2015-00:04:08 to 10-24-2015-01:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-24-2015-00:04:08 to 10-24-2015-01:04:08

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	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
109.66.148.22	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
222.186.21.84	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.21.84	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
212.7.209.9	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
185.82.201.17	147.237.77.216		dover.idf.il	ET DOS SSL Bomb DoS Attempt	1
81.192.139.152	147.237.77.61	Morocco	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
39.84.58.163	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.186.21.84	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
222.186.21.84	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.108.132.58	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
182.74.136.3	147.237.0.34	India	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
81.192.139.152	147.237.77.61	Morocco	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
27.154.180.206	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-24-2015-00:04:08 to 10-24-2015-01:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
173.84.92.52	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	92
105.235.128.134	Algeria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	81
86.192.193.118	France	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	75
87.69.247.184	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	73
108.45.80.52	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	67
149.78.154.69	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	67
5.29.28.173	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
188.247.75.203	Jordan	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	39
66.249.65.238	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
54.244.22.103	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	32
66.249.65.224	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
66.87.19.109	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	30
100.100.51.188		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	30
66.249.65.231	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	28
190.24.146.71	Colombia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
82.149.176.81	Germany	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
100.100.62.180		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	23
79.181.199.86	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
100.100.62.180		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
5.28.133.115	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
46.19.85.192	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	18
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
82.80.25.221	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
87.68.156.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
50.116.30.23	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
100.100.72.222		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
66.102.8.173	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.56.175		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
84.109.102.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
151.80.31.115	Italy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	SAM rule	drop	11
46.116.169.4	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
100.100.108.129		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.245	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
66.249.81.218	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
128.164.67.139	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
46.19.85.120	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
24.147.64.79	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
46.19.86.182	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
89.139.165.32	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
46.19.86.21	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
40.77.167.35	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7

10-24-2015-00:04:08 to 10-24-2015-01:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.247.184	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 87.69.247.184	Block	294
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2113-he/cogat.aspx	Block	84
68.180.230.97	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/589-he/patzar.aspx=	Block	84
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.231	Block	56
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
46.19.85.47	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.47	Block	42
46.19.85.47	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.47	Block	42
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	42
46.19.85.47	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 46.19.85.47	Block	42
46.19.85.47	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 46.19.85.47	Block	28
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	14
207.46.13.129	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14
2.54.129.167	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	14
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	14
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1129-he/kkkkkkk=73fe6783kkkkkkk_73fe6783	Block	14
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
207.46.13.129	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in aka.idf.il/ishurim/cityofficers/	None	14
41.234.17.46	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	14
89.138.199.205	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	14
188.143.232.40	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	14
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
46.19.85.47	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	14
141.212.122.160	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	14
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	14
188.165.15.121	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list2.htm	Block	14
81.223.254.34	Austria	147.237.77.74	law.idf.il	Unauthorized URL Access to /robots.txt	Block	14
66.249.64.249	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
46.19.85.47	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	14
157.55.39.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/sachar	Block	14
46.19.85.47	Israel	147.237.77.216	dover.idf.il	Unknown HTTP Request Method s=562aa551a093fa3b000 in URL	Block	14
195.154.226.90	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-content/	Block	14
87.69.247.184	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	14
167.114.64.100	Canada	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14

10-24-2015-00:04:08 to 10-24-2015-01:04:08