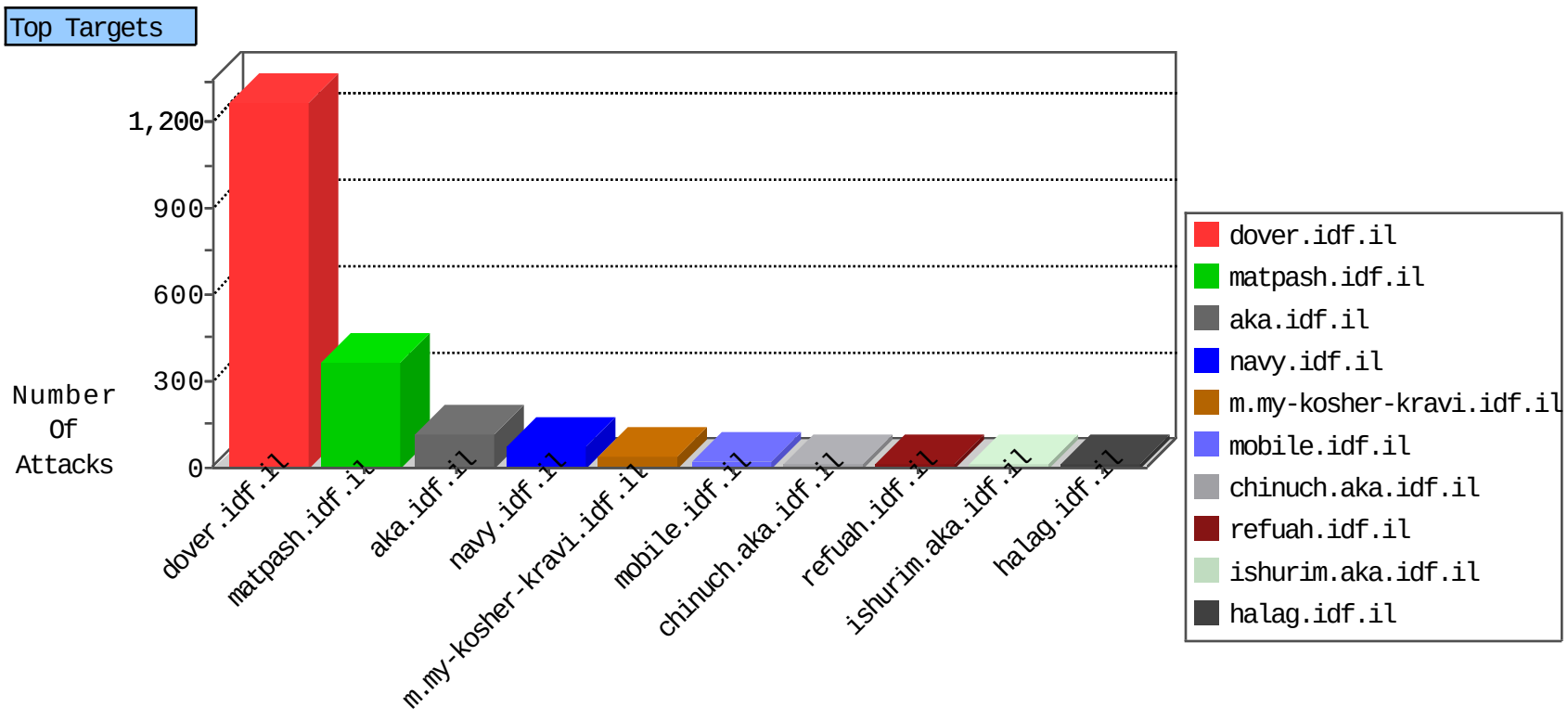
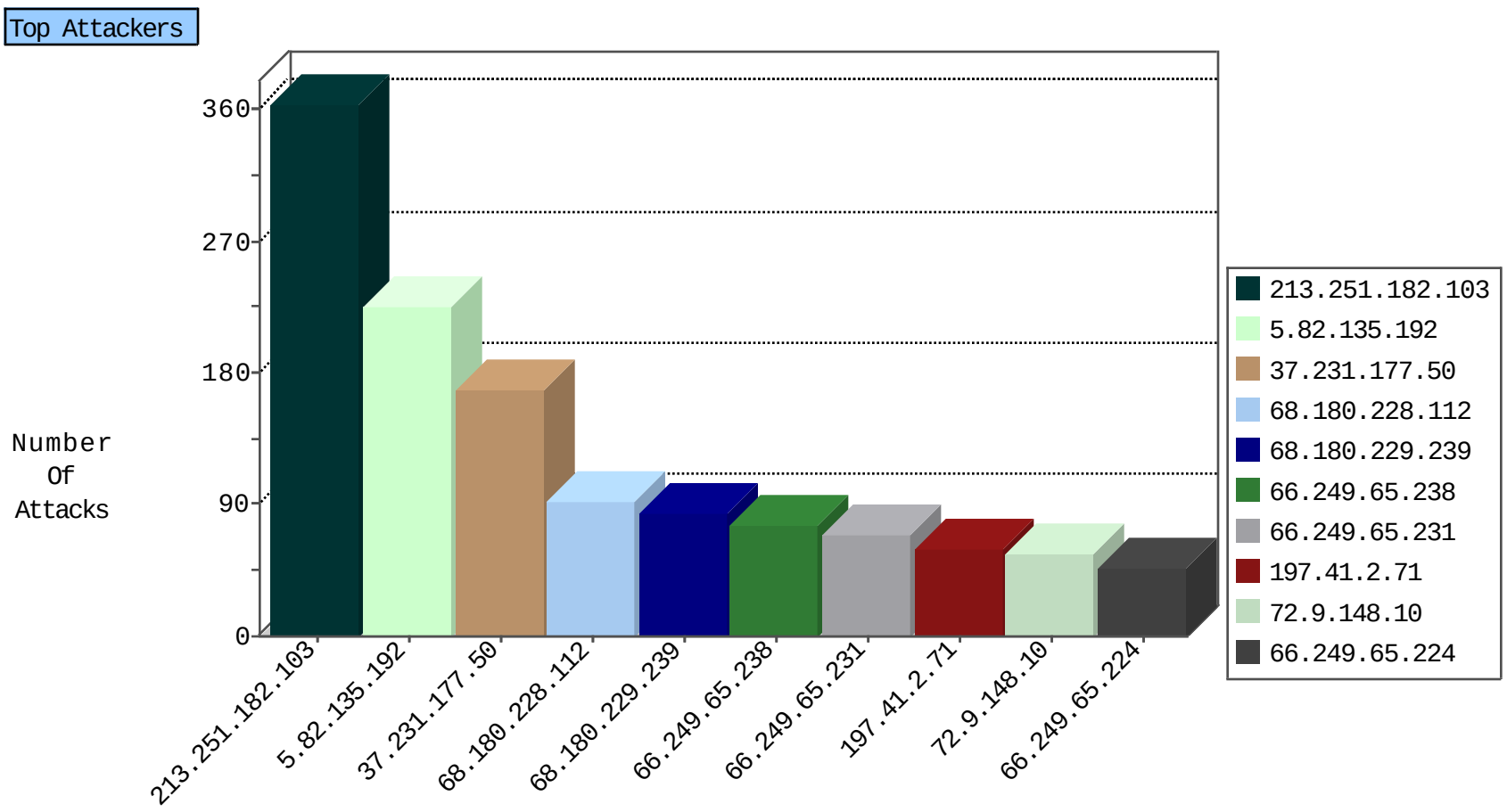
10-24-2015-05:04:00 to 10-24-2015-06:04:00

IDF Under Attack Daily Report





10-24-2015-05:04:00 to 10-24-2015-06:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.248.160.192	Netherlands	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.192	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.192	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
52.28.32.164	United States	147.237.76.197	e.himush.idf.il	JLM_Purple_Con_Limit_Https	drop	1
89.248.160.192	Netherlands	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
52.28.32.164	United States	147.237.76.199	e.nakchal.idf.il	JLM_Purple_Con_Limit_Https	drop	1
89.248.160.192	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

10-24-2015-05:04:00 to 10-24-2015-06:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-24-2015-05:04:00 to 10-24-2015-06:04:00

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	4
66.249.65.238	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
142.54.163.74	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
142.54.163.74	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
89.248.172.98	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.25.83	147.237.0.19	France	madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
142.54.163.74	147.237.77.61	United States	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
119.254.3.236	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
85.42.222.3	147.237.76.31	Italy	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
62.210.25.83	147.237.0.19	France	madim.atal.idf.i	ET SCAN NMAP -sS window 3072	1
222.186.42.11	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

10-24-2015-05:04:00 to 10-24-2015-06:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.82.135.192	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	225
37.231.177.50	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	169
197.41.2.71	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	40
96.51.240.165	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
79.183.38.132	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
50.162.178.25	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
52.91.173.216	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
40.77.167.36	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
208.54.36.255	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
75.126.221.55	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
108.200.226.186	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
40.77.167.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.228.34.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.116.169.4	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.65.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
101.183.79.112	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
173.54.17.35	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	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	5
201.21.145.40	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
193.169.234.5	Russian Federation	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
87.69.13.63	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
65.19.138.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
208.54.36.255	United States	147.237.77.216	dover.idf.il	drop		drop	4
109.200.30.154	United Kingdom	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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	4
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
63.227.45.6	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
208.54.36.255	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
157.55.2.160	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
208.54.36.255	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.67.34	United States	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
89.139.17.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.215.72.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

10-24-2015-05:04:00 to 10-24-2015-06:04:00

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	364
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	84
68.180.229.239	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	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
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	28
74.82.47.3	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/signals/atar/	Block	14
101.183.79.112	Australia	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 101.183.79.112	Block	14
67.19.79.218	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to /robots.txt	Block	14
54.179.134.216	Singapore	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	14
74.82.47.4	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	14
66.249.65.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-he/dover.aspx	Block	14
5.79.74.89	Netherlands	147.237.76.86	navy.idf.il	Suspicious Response Code	Block	14
141.212.122.160	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	14
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18775-he/dover.aspx	Block	14
85.64.202.120	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding -ZÂ©G;XV{{?)Qm;(5:_i[nxXkES5tKWCzY nY_xnV3l[J. in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	14
40.77.167.43	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
52.91.173.216	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
216.218.206.66	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	14
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	14
85.64.202.120	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	14
66.249.79.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	14
52.91.173.216	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jeninkilled/stn	Block	14
85.64.202.120	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 85.64.202.120	None	10

10-24-2015-05:04:00 to 10-24-2015-06:04:00