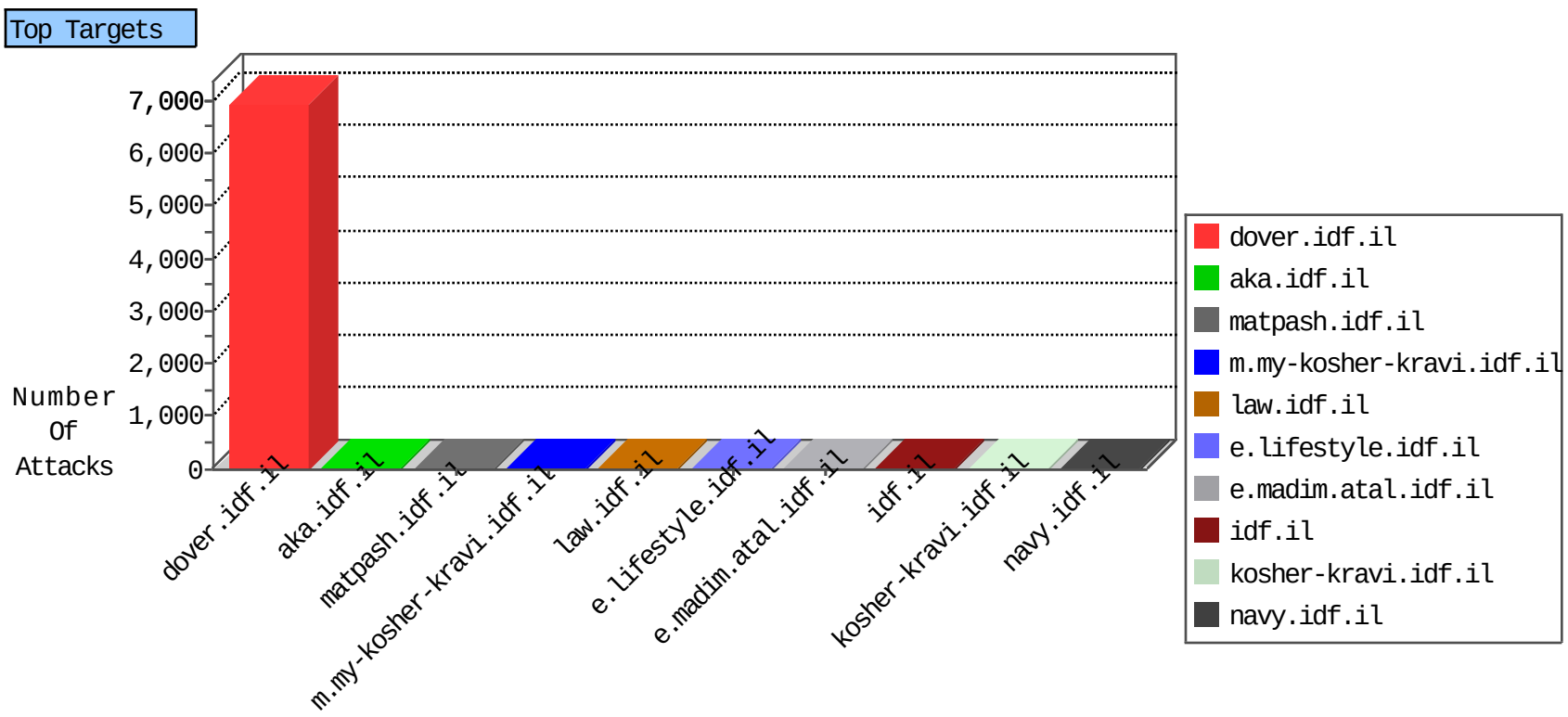
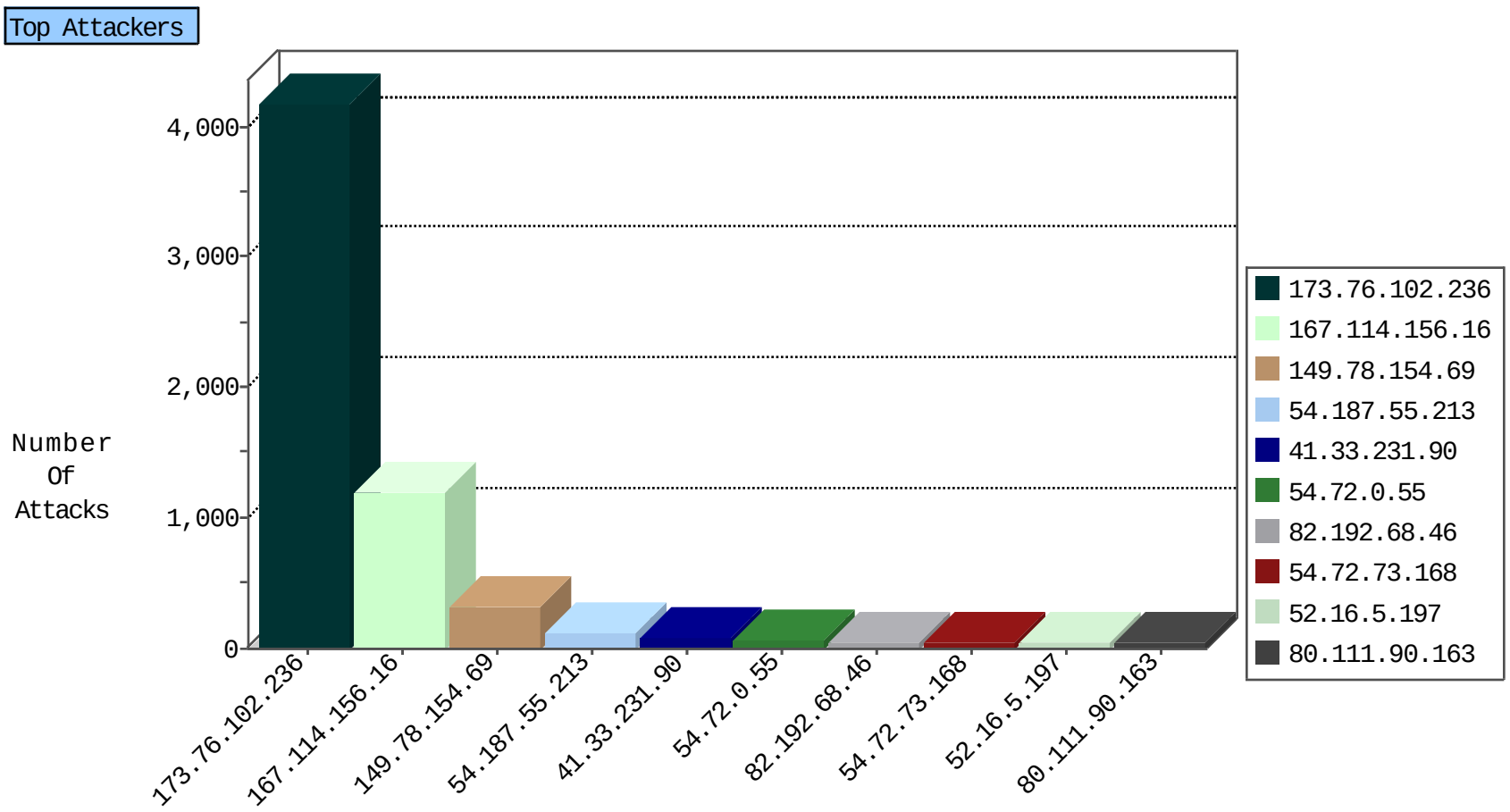
11-02-2015-04:04:00 to 11-02-2015-05:04:00

IDF Under Attack Daily Report



Top Target



Top Attackers

11-02-2015-04:04:00 to 11-02-2015-05:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2218
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	764
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
222.186.56.42	China	147.237.0.33	idf.il	Frk_Under_Attack_Con_Tcp	drop	1

11-02-2015-04:04:00 to 11-02-2015-05:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

11-02-2015-04:04:00 to 11-02-2015-05:04:00

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	11
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.67.122	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.13	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
5.8.66.101	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
173.1.121.85	147.237.0.33	United States	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
162.248.10.134	147.237.8.24	Canada	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
162.248.10.134	147.237.8.24	Canada	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
61.238.4.191	147.237.8.27	Hong Kong	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
5.8.66.101	147.237.0.15	Russian Federation	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
187.23.209.56	147.237.8.27	Brazil	e.madim.atal.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
173.1.121.85	147.237.0.15	United States	kosher-kravi.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
162.248.10.134	147.237.8.24	Canada	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
91.186.221.118	147.237.8.28	Iran, Islamic Republic of	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

11-02-2015-04:04:00 to 11-02-2015-05:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
173.76.102.236	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4180
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	328
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	122
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	52
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
80.111.90.163	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
216.177.129.204	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
116.255.24.1	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
27.122.115.41	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
94.76.21.74	Bahrain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
192.117.12.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
24.114.69.6	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	15
100.34.238.120	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
71.224.244.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
74.89.197.40	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
69.245.225.98	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.160.236.133	Israel	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
198.58.103.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
217.147.92.69	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
71.11.234.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
189.62.153.53	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.78.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.108	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
69.196.253.30	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
75.17.80.100	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.177.220.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
162.231.233.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.181.185.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.178.112.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

11-02-2015-04:04:00 to 11-02-2015-05:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.94.161.105	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	5
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	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
66.249.69.92	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
54.166.80.141	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
176.12.140.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
66.249.75.54	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
61.141.207.6	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
207.46.13.137	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1589- en/dover.aspx	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
66.249.69.76	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
46.117.164.60	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 46.117.164.60	None	1
66.249.75.62	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
213.139.52.53	Jordan	147.237.77.176	matpash.idf.il	Illegal HTTP Version	Block	1
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	1
66.249.69.84	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
54.82.82.197	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19372-he/idfgdover.aspx	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
5.254.97.108	Romania	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/'	Block	1
213.139.52.53	Jordan	147.237.77.176	matpash.idf.il	Malformed URL http/1.1	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1966-he/cogat.aspx	Block	1
66.249.69.84	Israel	147.237.77.74	law.idf.il	Parameter Type Violation SearchText in www.law.idf.il/163-6639-he/patzar.aspx	Block	1
54.144.225.126	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
84.110.36.99	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/ the official israeli naval website	Block	1
66.249.67.77	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
37.187.114.171	France	147.237.77.235	sviva.idf.il	Unauthorized URL Access to /xmii/illuminator	Block	1
213.139.52.53	Jordan	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method /4/2194.png in URL www.cogat.idf.ilhttp/1.1	Block	1

11-02-2015-04:04:00 to 11-02-2015-05:04:00