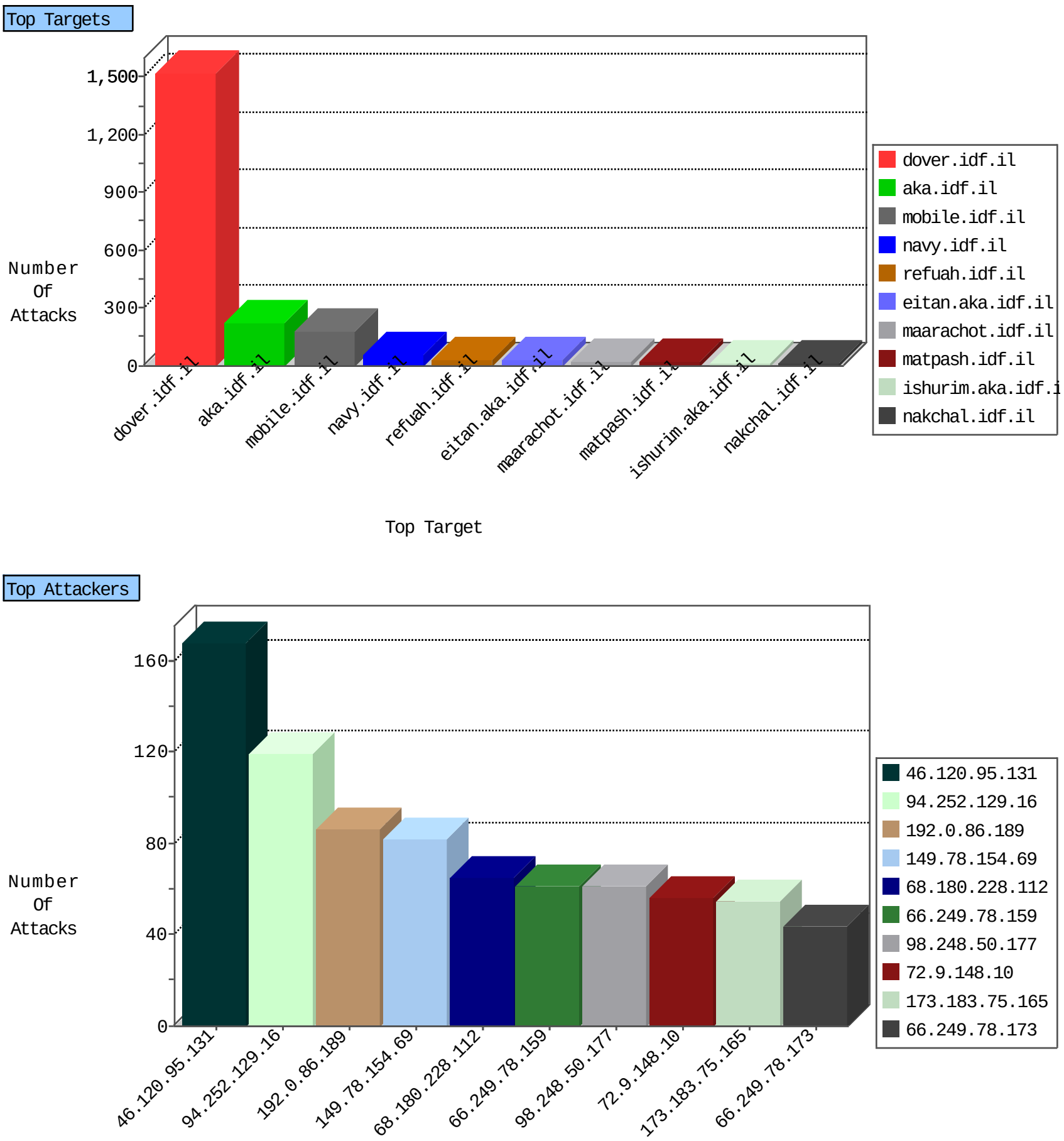
10-27-2015-06:04:08 to 10-27-2015-07:04:08

IDF Under Attack Daily Report



10-27-2015-06:04:08 to 10-27-2015-07:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.137.127	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
85.250.247.81	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
45.63.1.137		147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
96.44.156.198	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
45.63.1.137		147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
203.133.170.9	Korea, Republic of	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
5.102.254.115	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

10-27-2015-06:04:08 to 10-27-2015-07:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.194.11.113	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

10-27-2015-06:04:08 to 10-27-2015-07:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

10-27-2015-06:04:08 to 10-27-2015-07:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.252.129.16	Syrian Arab Republic	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	115
192.0.86.189	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	82
98.248.50.177	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	61
173.183.75.165	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	46
71.203.106.220	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
5.22.131.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
192.0.81.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
176.241.91.106	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
50.18.94.121	United States	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
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
95.86.65.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
80.246.133.222	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	18
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
36.81.160.81	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
176.228.142.125	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.67.137.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
212.76.127.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
77.125.155.210	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
185.58.201.28	Lebanon	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	13
109.67.181.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
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
54.241.198.78	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.78.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
67.174.242.236	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
92.224.205.102	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
85.250.247.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
207.198.101.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
172.56.31.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.12.137.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
219.83.38.14	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.65.2.183	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
80.246.133.222	Israel	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	8
192.0.86.129	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.76.112.48	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
104.174.161.135	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
108.27.77.123	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7

10-27-2015-06:04:08 to 10-27-2015-07:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.120.95.131	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	98
46.120.95.131	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 46.120.95.131	Block	70
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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info.asp	Block	42
82.166.98.205	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip-storage/files	Block	42
83.223.122.14	United Kingdom	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &y in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	28
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
157.55.39.196	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	14
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	14
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/17436.jpg	Block	14
79.177.14.104	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	14
157.55.39.209	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/klali.aspx	Block	14
46.120.203.175	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 46.120.203.175	Block	14
207.46.13.144	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/daily_	Block	14
157.55.39.209	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chinuch/faq/default.asp	None	14
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	14
212.199.57.198	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	14
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	14
5.175.25.171	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/qiyus/qeneral/default.a	Block	14
176.13.8.30	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	14
78.128.92.193	Bulgaria	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	14
66.249.75.120	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
85.64.81.239	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	14
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	14
184.105.139.67	United States	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	14
78.128.92.193	Bulgaria	147.237.77.235	sviva.idf.il	Unauthorized URL Access to 147.237.77.235/	Block	14

10-27-2015-06:04:08 to 10-27-2015-07:04:08