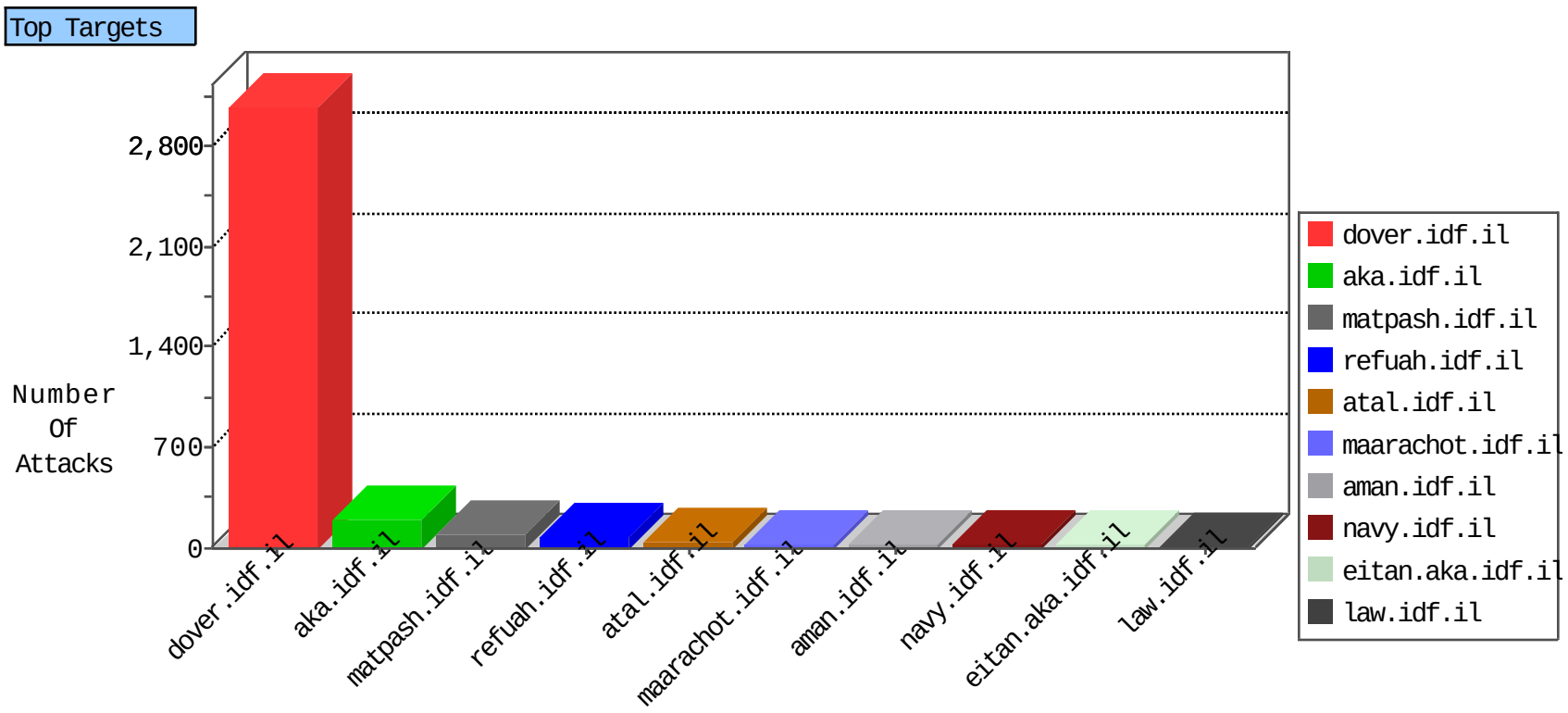
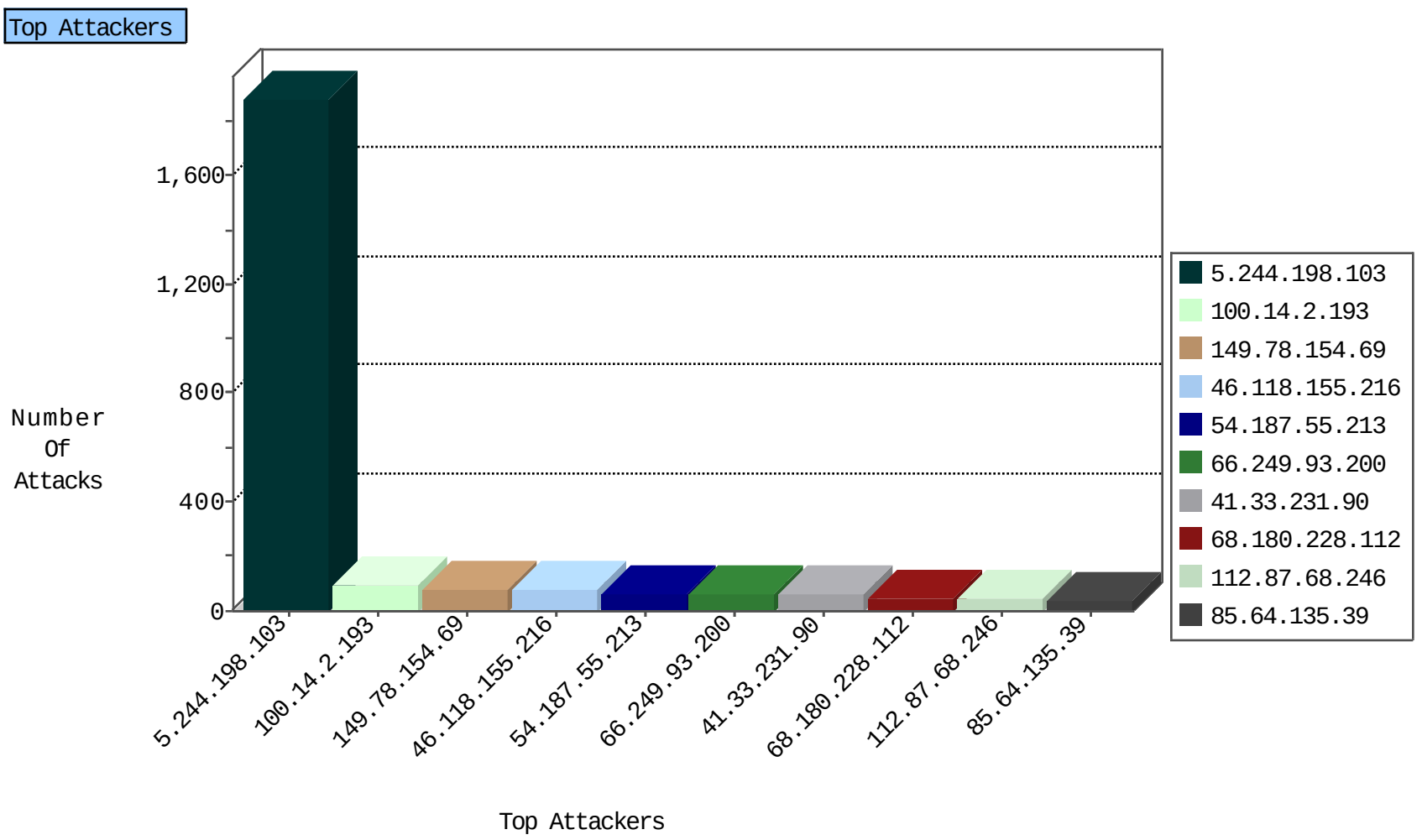
10-31-2015-07:04:01 to 10-31-2015-08:04:01

IDF Under Attack
Daily Report





10-31-2015-07:04:01 to 10-31-2015-08:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.244.198.103	Saudi Arabia	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2235
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1423
212.199.182.150	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1105
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	480
107.140.141.118	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	475
31.168.206.161	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
79.182.17.216	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
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
176.13.11.54	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
85.25.103.50	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

10-31-2015-07:04:01 to 10-31-2015-08:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

10-31-2015-07:04:01 to 10-31-2015-08:04:01

Top Attackers In IDS

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

10-31-2015-07:04:01 to 10-31-2015-08:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.244.198.103	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1761
100.14.2.193	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	92
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	62
66.249.93.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
5.244.198.103	Saudi Arabia	147.237.77.216	dover.idf.il	drop		drop	58
85.64.135.39	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
79.177.179.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
66.249.93.196	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
5.244.198.103	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	26
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	19
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.86.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
157.55.39.214	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.172.206.249	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
70.117.118.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
176.228.41.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
112.87.68.246	China	147.237.77.216	dover.idf.il	drop		drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
14.201.169.193	Australia	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
77.127.238.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
199.16.156.124	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
199.16.156.125	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
112.87.68.246	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	8
199.16.156.126	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
112.87.68.246	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
166.137.246.61	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
107.140.141.118	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
31.13.100.119	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
93.173.238.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
65.19.138.33	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.13.100.113	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.244.198.103	Saudi Arabia	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5

10-31-2015-07:04:01 to 10-31-2015-08:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	45
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
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	30
66.249.79.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/templates/sendtofriend/sendtofriend.aspx	Block	15
66.249.67.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
112.87.68.246	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	15
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/kapatz/citizencontact.aspx	Block	15
188.165.15.241	France	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	15
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	15
141.212.121.192	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	15
66.249.79.144	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2879.pdf	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/faq.aspx	Block	15
207.46.13.155	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	15
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
46.118.155.216	Ukraine	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	15
157.55.39.122	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	15
66.249.79.228	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9331-he/refuah.aspx	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	15
5.244.198.103	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	15
213.57.160.27	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 104 cookies	Block	15
79.181.27.142	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	15
66.249.69.76	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	15
52.23.156.32	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
176.228.41.8	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	15
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8935-he/refuah.aspx	Block	15
66.249.67.143	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	15
14.201.169.193	Australia	147.237.76.200	eitan.aka.idf.il	Cookie Tampering on cookie __atssc: Expected facebook;1, Observed facebook;2	None	15
84.228.73.150	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	15
66.249.69.97	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1245-he/atal.aspx	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	15
182.58.106.57	India	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method COOK in URL www.tikshuv.idf.il/1048-7535-he/tikshuv.aspx	Block	15

10-31-2015-07:04:01 to 10-31-2015-08:04:01