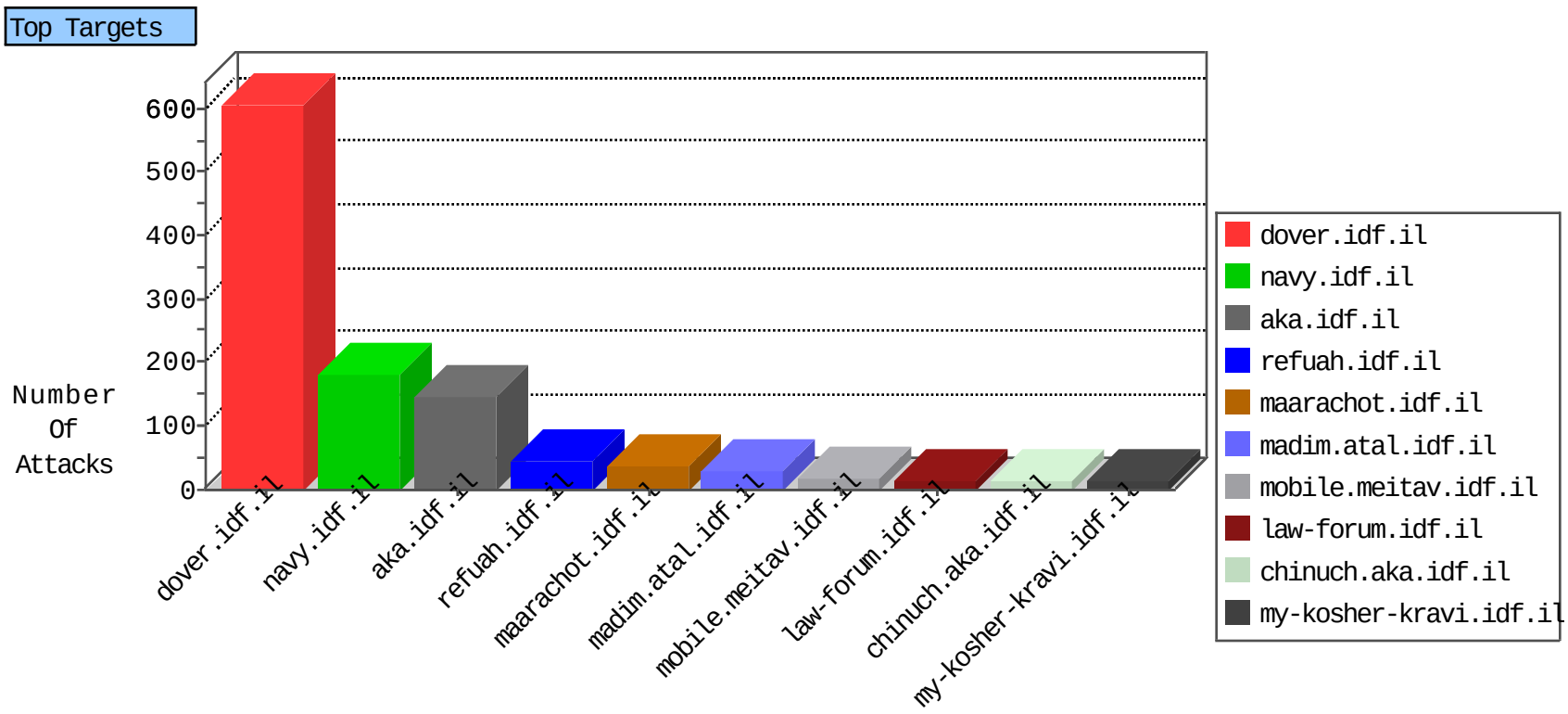
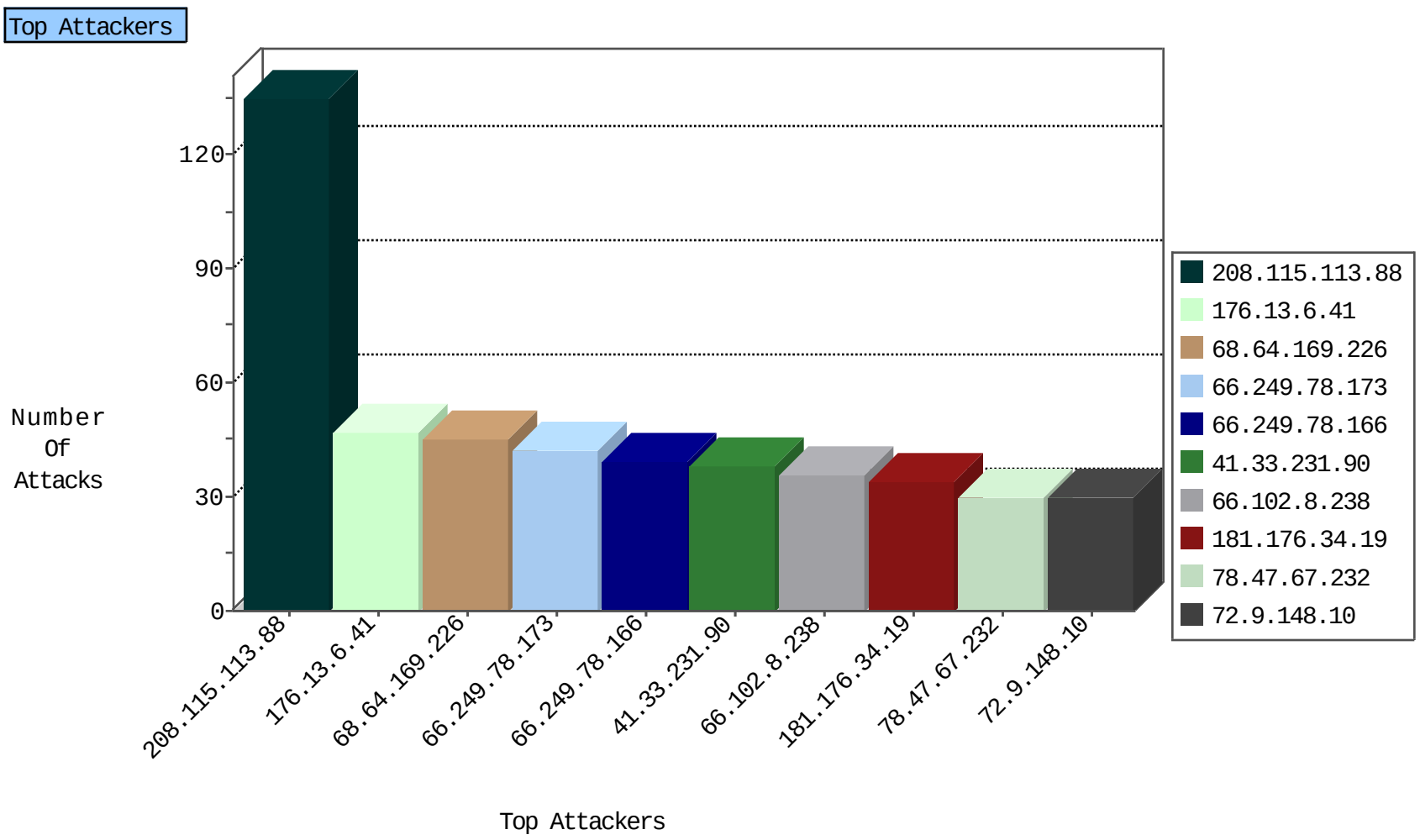
10-31-2015-04:04:06 to 10-31-2015-05:04:06

IDF Under Attack
Daily Report

Top Targets



Top Attackers



10-31-2015-04:04:06 to 10-31-2015-05:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.67.34	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	7237
66.249.67.27	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	73
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
17.142.152.110	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
85.25.103.50	Germany	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

10-31-2015-04:04:06 to 10-31-2015-05:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
94.73.145.90	Turkey	147.237.72.166	aka.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	20

10-31-2015-04:04:06 to 10-31-2015-05:04:06

Top Attackers In IDS

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

10-31-2015-04:04:06 to 10-31-2015-05:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.6.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
66.102.8.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
181.176.34.19	Peru	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
66.249.78.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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	24
17.142.152.85	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.102.8.243	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
17.142.152.68	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.102.8.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
17.142.152.72	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
17.142.152.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
17.142.152.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
17.142.152.111	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
66.249.78.51	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
17.142.152.110	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.87.64.60	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
131.253.25.181	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.130.82	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
17.142.152.94	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
86.190.118.194	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.102.8.233	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
17.142.152.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.54.47.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.78.37	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.214	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
65.19.138.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.102.8.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
149.88.230.134	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
157.55.39.245	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
84.111.38.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
151.80.31.112	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.67.91	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.201	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
89.234.157.254	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.247.231	United States	147.237.8.50	e.tikshuv.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
157.55.39.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

10-31-2015-04:04:06 to 10-31-2015-05:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	120
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
78.47.67.232	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	30
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/booklets.aspx	Block	15
192.92.196.71	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	15
68.64.169.226	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	15
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	15
66.249.67.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1158-he/chinuch.aspx	Block	15
151.80.31.112	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	15
66.249.79.228	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8847-he/refuah.aspx	Block	15
66.249.67.134	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/0/112800.pdf	Block	15
207.46.13.113	United States	147.237.72.166	aka.idf.il	Unknown Parameter sorderby in aka.idf.il/iturim/asp/wars.asp	None	15
68.64.169.226	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	15
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19916-he/idfgdover.aspx	Block	15
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
176.126.252.12	Romania	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	15
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8944-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/pdf/files/2/109692.pdf	Block	15
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18457-he/dover.aspx	Block	15
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
178.255.215.87	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	15
66.249.79.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8873-he/refuah.aspx	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
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/edim/library/library.asp	Block	15
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	15
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	15
184.105.139.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	15
68.64.169.226	United States	147.237.0.19	madim.atal.idf.il	Unauthorized HTTP Method	Block	15
66.249.78.66	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	15
66.249.65.251	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/terms.aspx	Block	15
141.212.121.192	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	15

10-31-2015-04:04:06 to 10-31-2015-05:04:06