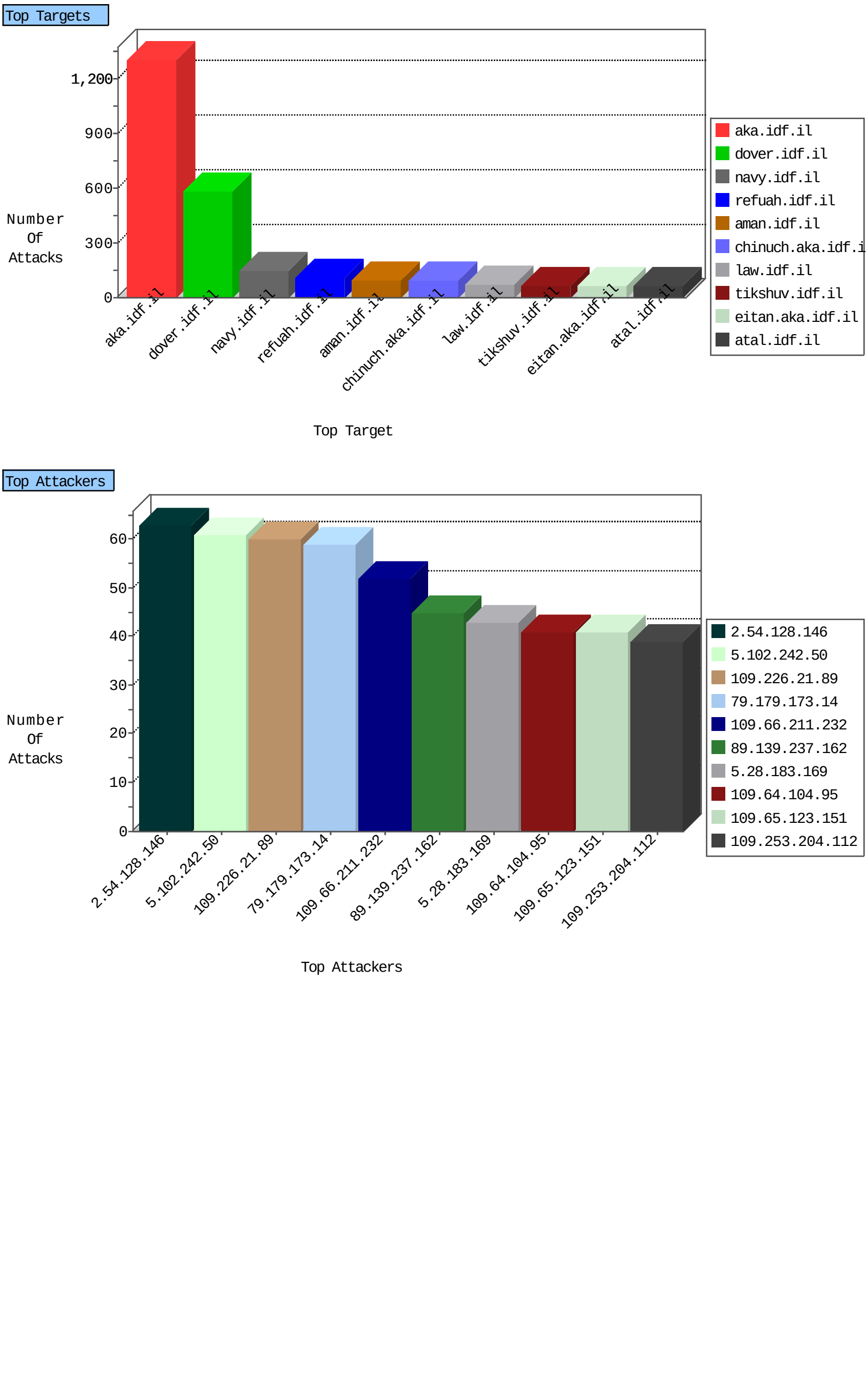
02-22-2016-22:04:06 to 02-22-2016-23:04:06

IDF Under Attack
Daily Report



02-22-2016-22:04:06 to 02-22-2016-23:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.208.206.204	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
107.150.60.75	United States	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
180.97.106.37	China	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
107.150.60.78	United States	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
180.97.106.162	China	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
173.208.206.203	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
180.97.106.162	China	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
107.150.33.62	United States	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1

02-22-2016-22:04:06 to 02-22-2016-23:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.34.222	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
46.137.81.122	Ireland	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
176.13.6.14	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.137.81.122	Ireland	147.237.76.86	navy.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
46.137.81.122	Ireland	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
106.120.173.130	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
46.137.81.122	Ireland	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
87.68.78.11	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
152.115.70.227	Denmark	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
87.71.23.36	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
136.243.103.156	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
211.23.251.92	Taiwan	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

02-22-2016-22:04:06 to 02-22-2016-23:04:06

Top Attackers In IDS

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

02-22-2016-22:04:06 to 02-22-2016-23:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.226.21.89	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
5.102.242.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.66.211.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	29
2.54.27.151	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
5.102.242.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
87.70.4.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
2.54.128.146	Israel	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	21
2.54.128.146	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	21
2.54.128.146	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
79.177.112.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
5.22.130.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
79.179.173.14	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
79.181.223.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
85.65.116.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
79.181.223.206	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
85.65.116.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
79.179.173.14	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	17
5.28.183.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	17
89.139.237.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
109.66.211.232	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
109.64.104.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
109.65.123.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
40.77.167.55	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
40.77.167.55	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
2.54.25.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.65.123.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	14
159.203.89.254	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
89.139.237.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
109.64.104.95	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
5.28.183.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
89.139.143.255	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
2.54.99.242	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
77.126.82.93	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
79.179.173.14	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	12
2.52.168.102	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
79.179.173.14	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
79.179.221.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
208.109.97.62	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
185.120.126.67		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
109.253.204.112	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence		monitor	11
2.52.10.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
2.52.10.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
108.21.51.69	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
84.94.181.155	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence		monitor	10
89.139.237.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.152.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
208.109.97.62	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
93.173.24.148	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence		monitor	10

02-22-2016-22:04:06 to 02-22-2016-23:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.125.3	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
109.66.211.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
199.203.77.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
77.126.151.24	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1

02-22-2016-22:04:06 to 02-22-2016-23:04:06