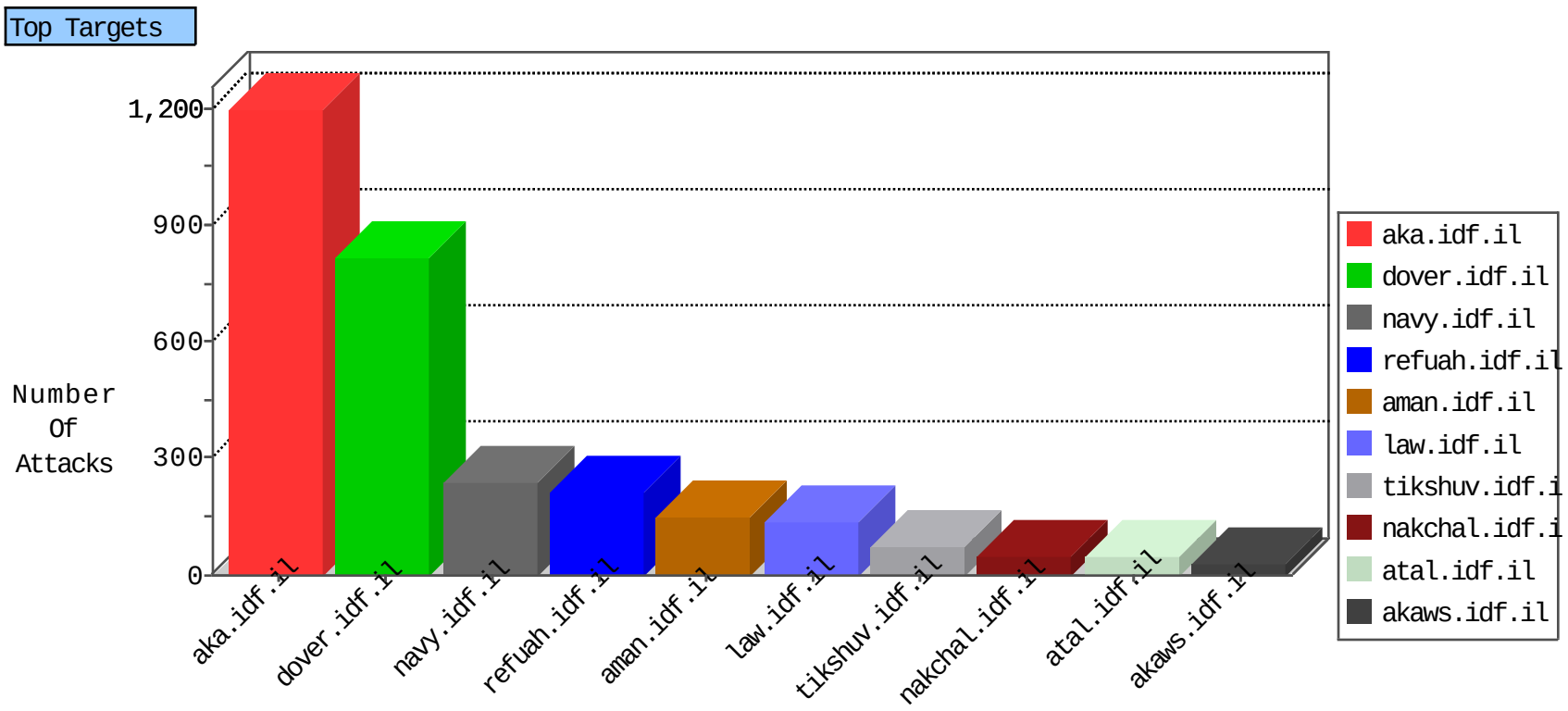
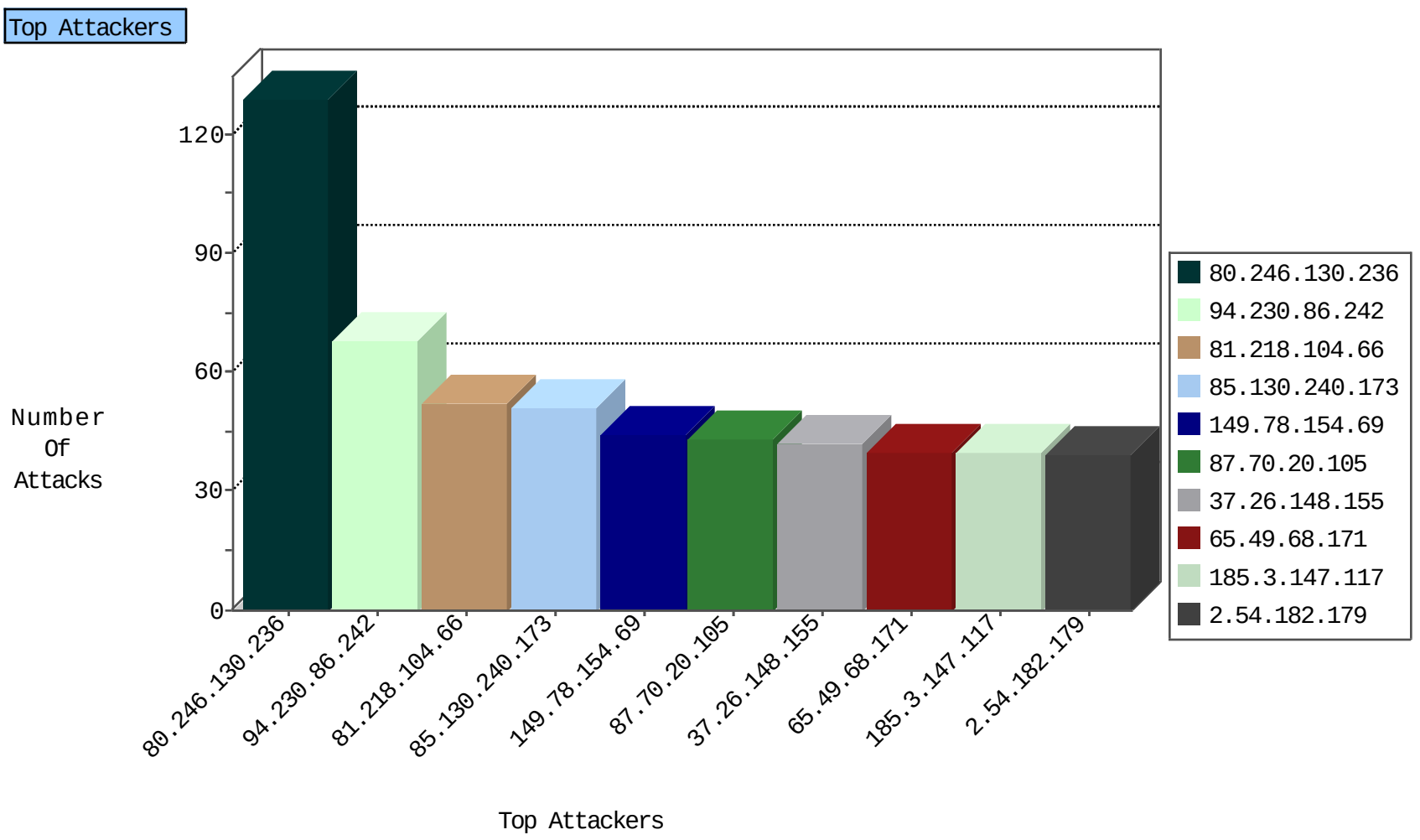
02-22-2016-23:04:00 to 02-23-2016-00:04:00

IDF Under Attack Daily Report





02-22-2016-23:04:00 to 02-23-2016-00:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
115.239.228.10	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Purple_Con_Limit_Http	drop	3
115.239.228.10	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
117.32.75.18	China	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.93	Switzerland	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

02-22-2016-23:04:00 to 02-23-2016-00:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.130	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
2.54.9.155	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.254.131.246	United Kingdom	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
51.254.131.246	United Kingdom	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
109.253.129.200	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

02-22-2016-23:04:00 to 02-23-2016-00:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
31.168.172.144	147.237.77.205	Israel	prisha.idf.il	SERVER-WEBAPP Mambo upload.php access	1
31.168.172.144	147.237.77.19	Israel	law-forum.idf.il	SERVER-WEBAPP Mambo upload.php access	1
31.168.172.144	147.237.0.34	Israel	tikshuv.idf.il	SERVER-WEBAPP Mambo upload.php access	1
31.168.172.144	147.237.77.234	Israel	halag.idf.il	SERVER-WEBAPP Mambo upload.php access	1
31.168.172.144	147.237.77.170	Israel	maarachot.idf.il	SERVER-WEBAPP Mambo upload.php access	1
31.168.172.144	147.237.76.200	Israel	eitan.aka.idf.il	SERVER-WEBAPP Mambo upload.php access	1

02-22-2016-23:04:00 to 02-23-2016-00:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.130.236	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	128
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
185.3.147.117	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
85.65.95.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
65.49.68.171	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	22
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	22
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
37.26.148.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
37.26.148.155	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	21
84.109.49.196	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
84.109.49.196	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
63.141.204.197	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
81.218.104.66	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
81.218.104.66	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
109.66.15.111	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
109.66.15.111	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
94.230.86.242	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
81.218.104.66	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
79.178.115.36	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
149.88.36.60	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
94.230.86.242	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
87.70.20.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
85.130.240.173	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
85.130.240.173	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
107.150.24.150	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
46.116.255.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
79.176.17.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.121.252.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
87.71.1.4	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.108.100.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
79.176.17.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
84.108.100.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
185.120.125.59		147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.90	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	12
2.52.161.27	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
87.70.20.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.116.255.77	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
79.176.30.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
185.120.126.67		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
82.166.68.171	Israel	147.237.0.35	akaws.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
5.144.63.115	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
149.88.243.39	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
149.88.243.39	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
185.120.126.67		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.85.43	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.52.36.233	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.148	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10

02-22-2016-23:04:00 to 02-23-2016-00:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-22-2016-23:04:00 to 02-23-2016-00:04:00