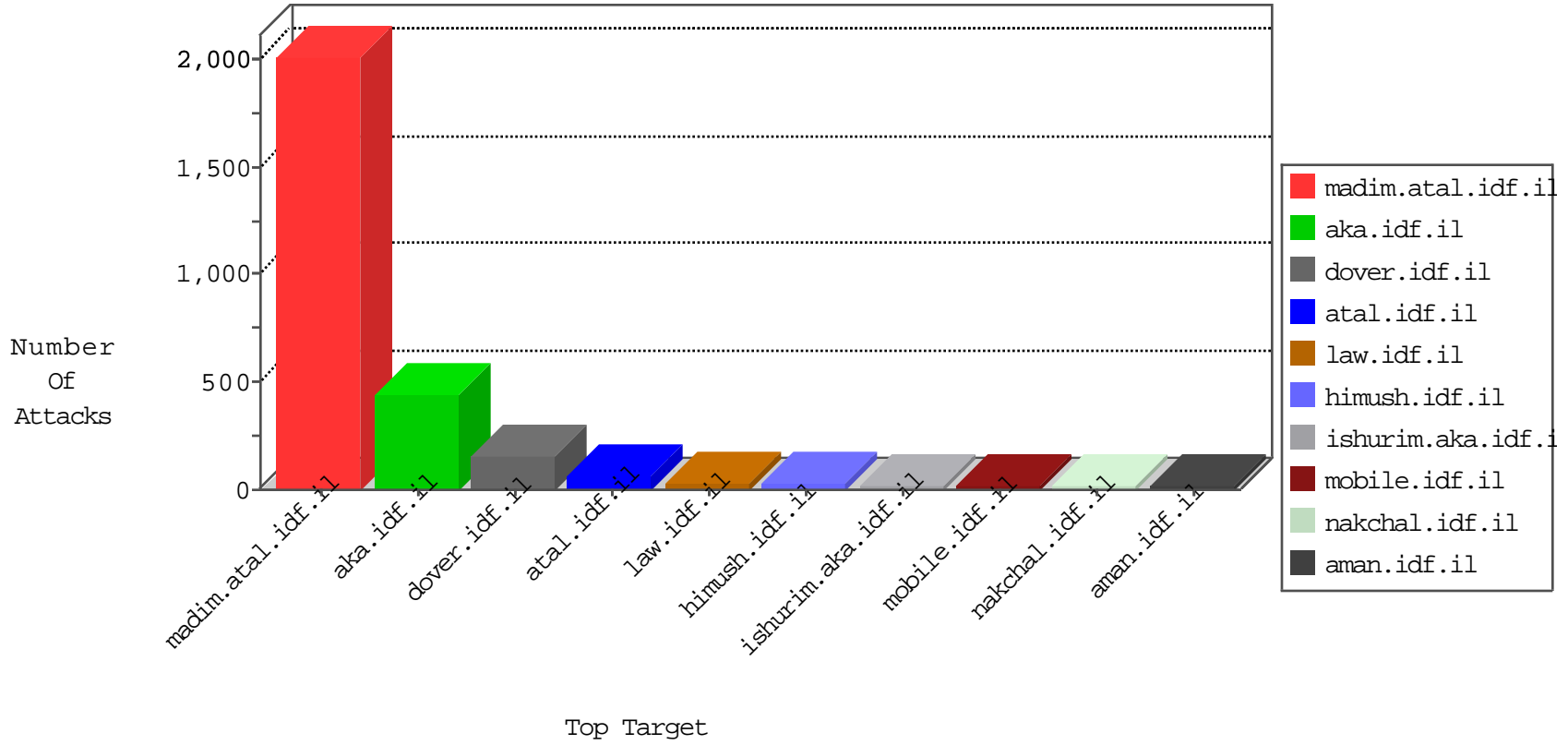


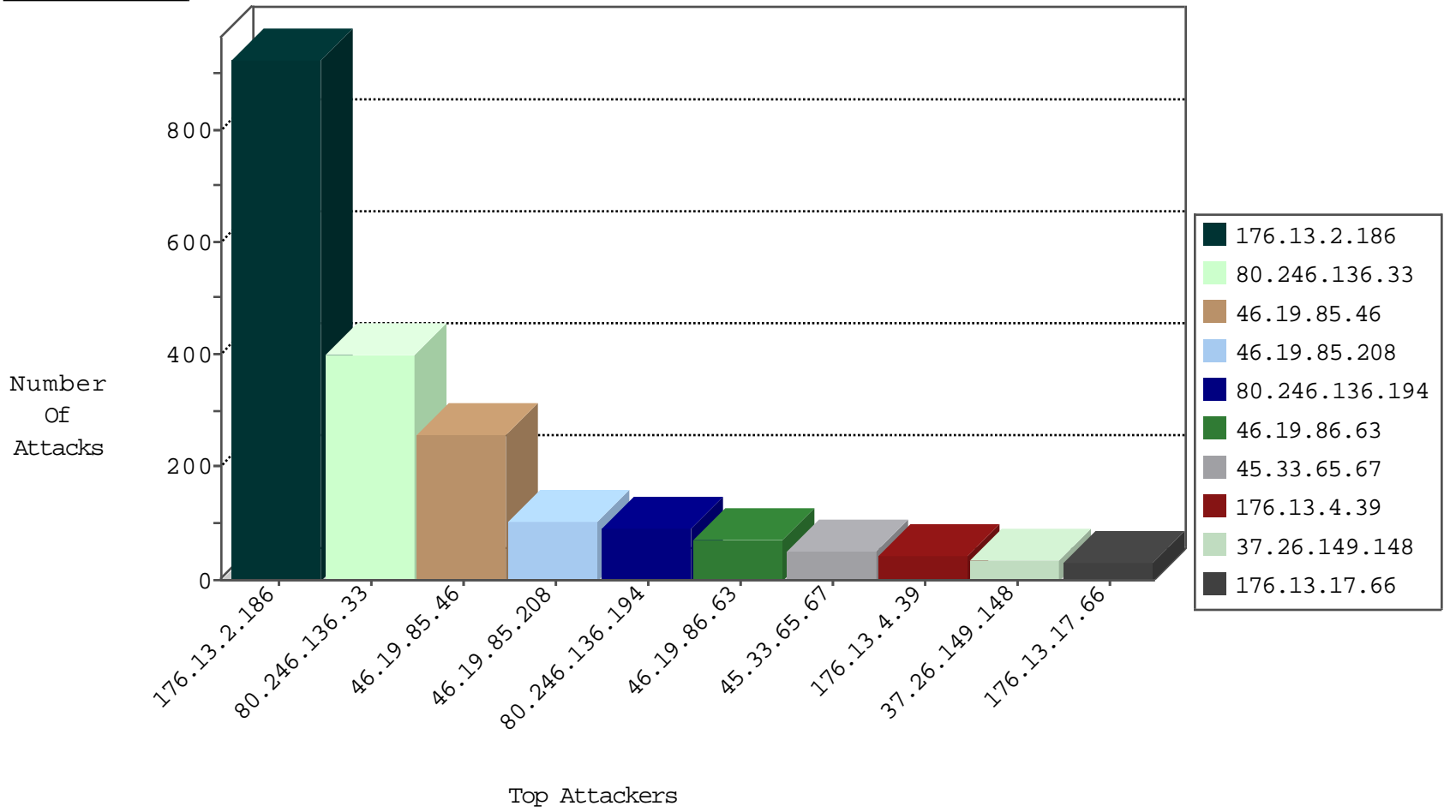
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.91.28.60	United States	147.237.76.31	nakchal.idf.il	block-sp-traf1	drop	1
123.151.42.61	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1

02-09-2016-13:04:06 to 02-09-2016-14:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
78.173.195.2	Turkey	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
------------------	----------------	------------------	------	-----------	-------

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.81.175	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	23
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
149.88.252.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
45.33.65.67		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
213.8.41.145	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
72.9.148.10	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	15
45.33.65.67		147.237.72.166	aka.idf.il	drop		drop	13
79.182.70.84	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.133.79	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.249.81.183	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	12
79.177.24.99	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.37.98.236	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
62.0.200.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
45.33.65.67		147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
45.33.65.67		147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
80.246.133.79	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
109.64.193.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
5.11.40.7	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.176.96.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.200.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
194.90.76.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.180.2.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.179.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.2.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.94.223.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.130.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.166.23.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.32.203.181	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.86.1	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.177.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
199.203.8.2	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.54.159.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
66.249.81.183	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
194.90.76.218	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
46.117.101.80	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.81.183	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
62.0.207.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
80.179.35.45	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
5.102.195.86	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
41.37.98.236	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
66.249.81.183	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.66.81.207	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
188.120.148.27	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.15.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.2.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	579
80.246.136.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	232
176.13.2.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	216
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	136
176.13.2.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	130
80.246.136.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	121
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.46	Block	117
80.246.136.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
46.19.85.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
46.19.86.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
80.246.136.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	47
176.13.4.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	43
176.13.17.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
37.26.149.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
46.19.85.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
185.32.179.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
109.253.195.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
78.173.195.2	Turkey	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 78.173.195.2	Block	5
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	Block	4
176.13.11.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
78.173.195.2	Turkey	147.237.72.166	aka.idf.il	PHP Attempt	Block	4
62.219.195.38	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
176.13.5.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
78.173.195.2	Turkey	147.237.72.166	aka.idf.il	Multiple Admin Blocking from 78.173.195.2	Block	3
109.253.212.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.199.57.194	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
176.13.22.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.15.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
89.139.60.36	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	3
37.26.149.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.1	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.149.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.9.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
46.19.86.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.143.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.1.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.197.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.65	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
157.55.39.192	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
94.159.191.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sacher	Block	1
193.188.70.138	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
78.173.195.2	Turkey	147.237.72.166	aka.idf.il	Admin Blocking	Block	1
109.253.211.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ctl100\$cphMain\$cphSachar\$ctl109 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
217.132.13.245	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
46.19.85.46	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.46	Block	1
212.143.134.129	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter amp;f in www.eitan.aka.idf.il/templates/sendtofriend/sendtofriend.aspx	None	1
87.69.123.100	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	1
79.178.142.219	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.154.37.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1