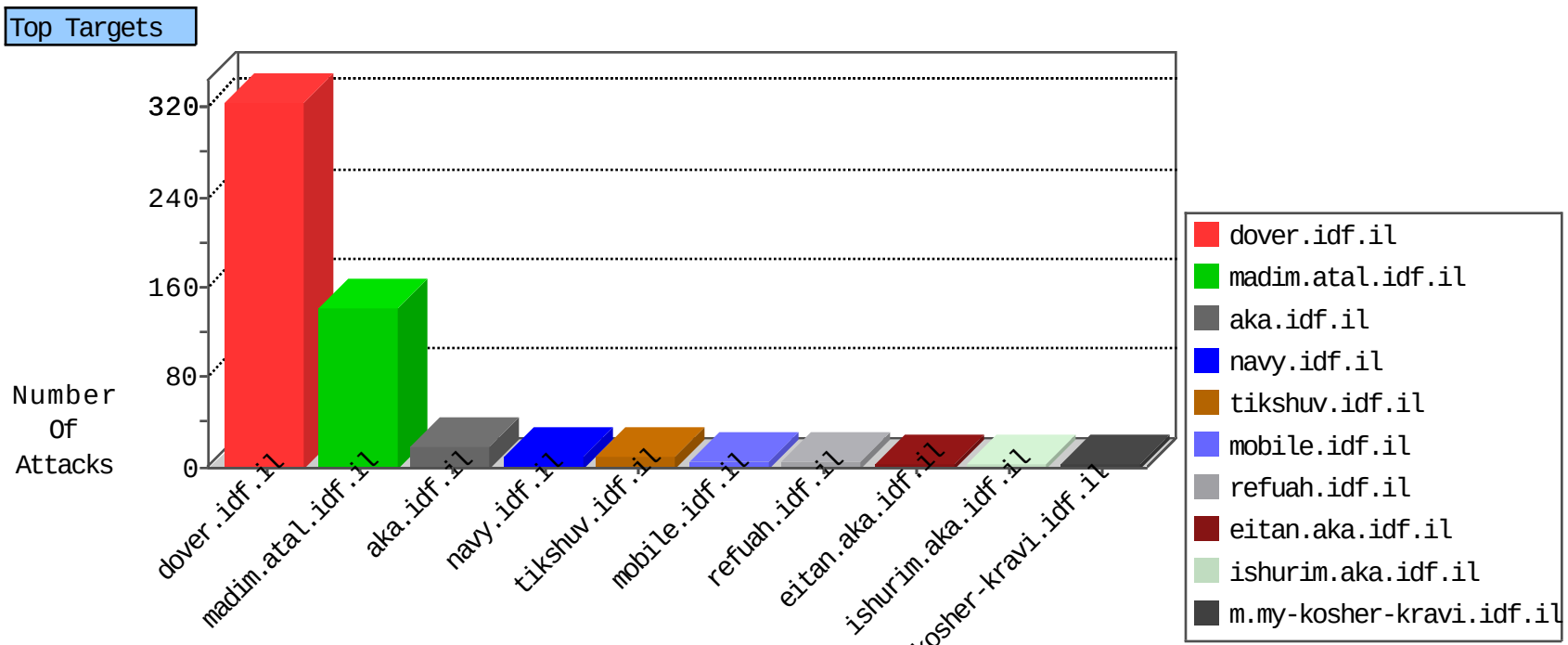
08-22-2016-08:04:09 to 08-22-2016-09:04:09

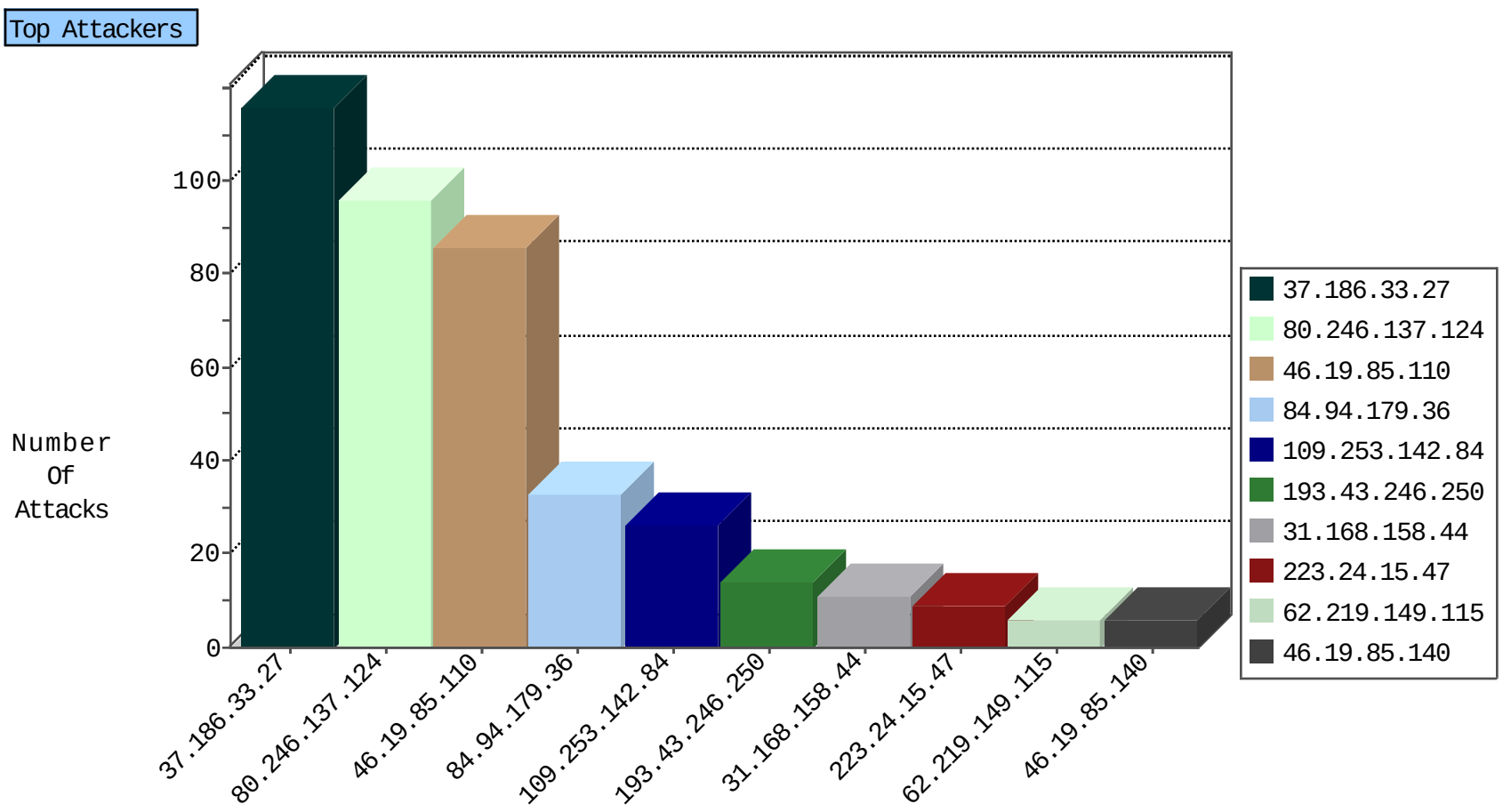
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-22-2016-08:04:09 to 08-22-2016-09:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.161.156	Israel	147.237.72.167	ishurim.aka.idf.il	Black List	drop	3
120.132.50.135	China	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
89.248.168.21	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
89.248.168.21	Netherlands	147.237.76.42	refuah.idf.il	Black List	drop	1

08-22-2016-08:04:09 to 08-22-2016-09:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.165.197.142	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.255.65.75	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
89.248.167.131	Netherlands	147.237.0.19	madim.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
198.20.99.130	Netherlands	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
51.255.65.4	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-22-2016-08:04:09 to 08-22-2016-09:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	3

08-22-2016-08:04:09 to 08-22-2016-09:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.186.33.27	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	116
46.19.85.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	85
84.94.179.36	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
31.168.158.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
84.94.179.36	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	10
223.24.15.47	Thailand	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
62.219.149.115	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.176.84.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
81.218.118.126	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.111.141.73	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
128.242.249.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
82.81.49.79	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.93.107	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.66.159.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.167.64	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.60.104.152	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
31.146.125.61	Georgia	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
82.213.48.30	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
220.181.51.77	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.93.111	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
220.181.51.81	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
123.116.242.133	China	147.237.0.200	m4u.idf.il	drop		drop	1
220.181.51.109	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
220.181.51.75	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
220.181.51.76	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
108.170.187.196	Canada	147.237.76.34	yohalan.idf.il	drop		drop	1
176.13.236.242	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

08-22-2016-08:04:09 to 08-22-2016-09:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.137.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
109.253.142.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
77.138.177.3	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	4
37.26.149.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.133	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.30.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.167.128	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
77.138.177.3	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.177.3	Block	2
185.27.105.131	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
10.152.50.62		147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	2
82.166.244.220	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.53.142.28	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
185.120.126.32	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.115	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Parameter Name Gb&T907@)DKd&f^z^H!1kR[[#28]]{	Block	1
24.107.226.62	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
109.226.48.178	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/step3.aspx	None	1
77.237.138.202	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
46.19.85.110	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
2.53.164.249	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.66.117	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	1
78.19.224.39	Ireland	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
2.53.184.71	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/ui/ui.datepicker.js	Block	1
31.210.186.173	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.5.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
5.22.135.174	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/bottomcap.gif	Block	1
2.53.41.28	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
79.182.6.214	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
66.249.66.115	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	1

08-22-2016-08:04:09 to 08-22-2016-09:04:09