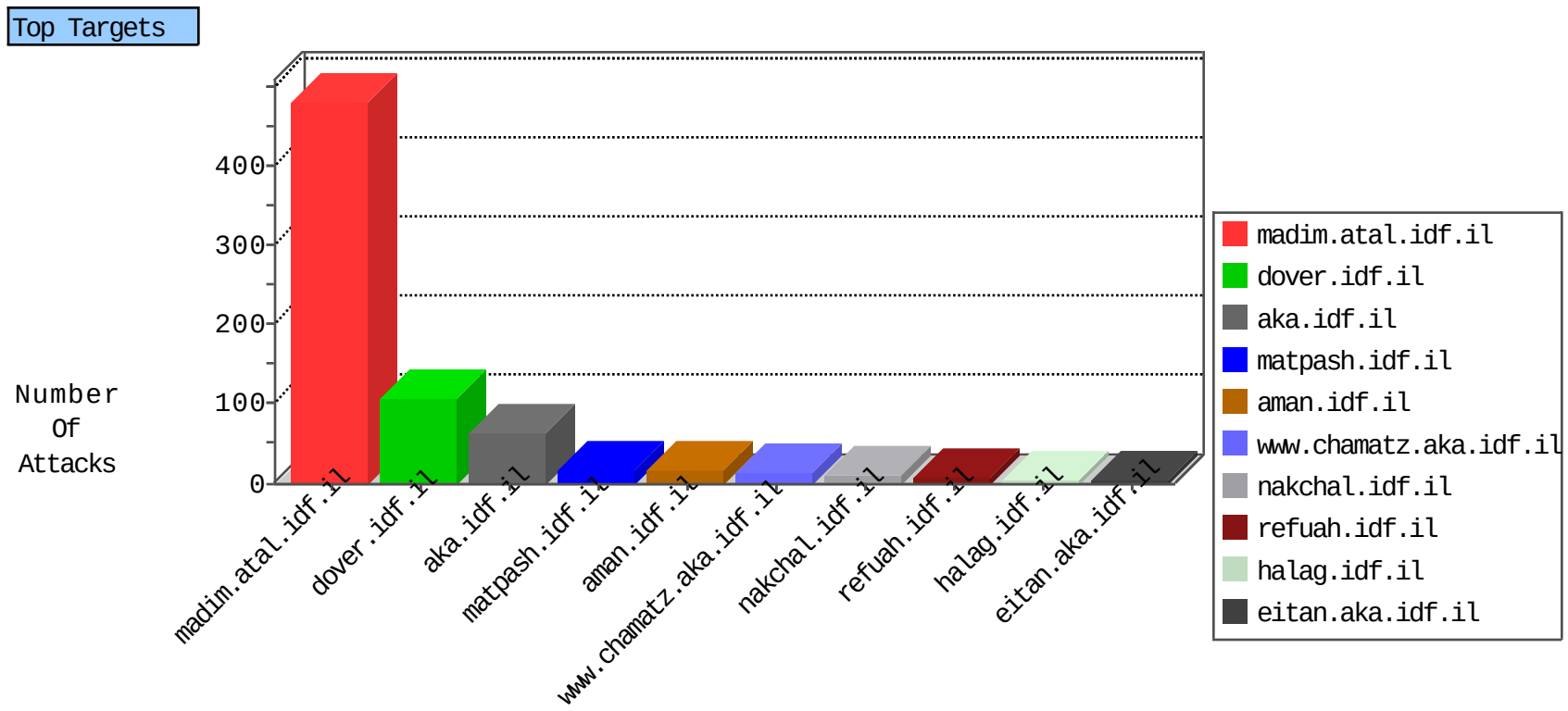
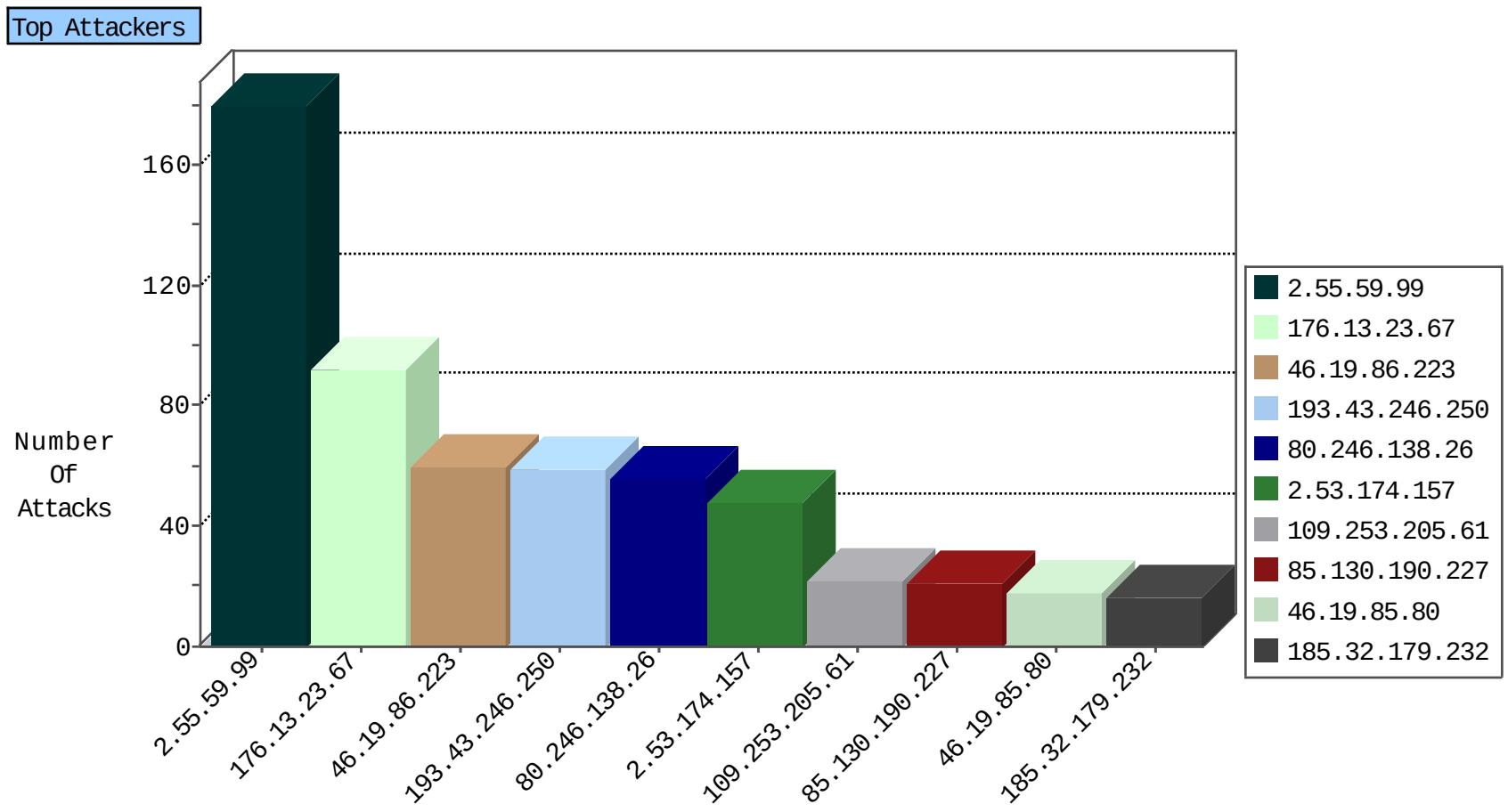
08-23-2016-11:04:07 to 08-23-2016-12:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



08-23-2016-11:04:07 to 08-23-2016-12:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.166.177	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	1
163.172.227.198	United Kingdom	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1
58.183.223.151	Japan	147.237.76.86	navy.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.197	e.himush.idf.il	Black List	drop	1
79.178.131.83	Israel	147.237.72.166	aka.idf.il	Black List	drop	1

08-23-2016-11:04:07 to 08-23-2016-12:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

08-23-2016-11:04:07 to 08-23-2016-12:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
5.22.134.202	147.237.76.200	Israel	eitan.aka.idf.il	Xenu Link Sleuth User Agent	3
5.102.198.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.105.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.236.194.161	147.237.72.167	Czech Republic	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
2.55.55.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.97.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.52.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.2.237	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.138.15.186	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
58.218.204.245	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
212.179.146.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	1
31.168.99.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.113.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.208.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.230.85.254	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.22.134.202	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	1
84.95.206.230	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.153.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.109.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.138.16.183	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.76.106	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.26.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.178.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.169	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.144.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

08-23-2016-11:04:07 to 08-23-2016-12:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
109.253.205.61	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
85.130.190.227	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	14
91.195.162.254	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
62.74.9.248	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
85.130.190.227	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.13.8.21	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
109.253.210.170	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
85.113.123.146	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.23.193	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
85.130.190.227	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
62.0.210.1	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
82.213.15.214	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
176.13.8.90	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
109.253.203.109	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
79.178.117.182	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
81.177.127.249	Russian Federation	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
176.13.229.106	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
82.81.50.127	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.245.123	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1

08-23-2016-11:04:07 to 08-23-2016-12:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.59.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	180
176.13.23.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
46.19.86.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
80.246.138.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	56
2.53.174.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
46.19.85.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
185.32.179.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
113.120.110.198	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 113.120.110.198	Block	9
81.218.241.25	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	6
212.143.135.92	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	5
113.120.110.198	China	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	4
46.19.85.16	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
2.53.3.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.180.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.229.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.205.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
80.246.138.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.243.40.98	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.194	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1116-he/ãƒâ€”ã,â¦ãƒâ€”ã¢â,¬â•	Block	1
37.26.146.247	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
109.65.154.92	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
212.143.135.92	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/2/	Block	1
79.176.140.65	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	1
192.243.55.137	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/tizmoret/gallery	Block	1
68.180.230.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
109.65.154.92	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.176.140.65	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/4	Block	1
46.120.69.43	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
192.243.55.138	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	1
5.22.134.202	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/main/	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/topcap.gif	Block	1
212.76.110.6	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl51 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
77.124.28.119	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
212.179.42.241	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
79.179.36.159	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1880	Block	1
192.243.55.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
113.120.110.198	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.asp	Block	1
5.22.134.202	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for www.eitan.aka.idf.il/894-he/eitan.aspx	None	1
77.138.192.71	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
176.13.250.172	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.85.247	Israel	147.237.76.31	nakchal.idf.il	Malformed URL	Block	1
109.253.210.13	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
212.243.40.98	Switzerland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
80.55.52.130	Poland	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/	Block	1
66.249.79.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1810-he/dover.aspx	Block	1
194.114.146.227	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 194.114.146.227	Block	1
124.188.0.88	Australia	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/haredim/general.aspx	Block	1

08-23-2016-11:04:07 to 08-23-2016-12:04:07