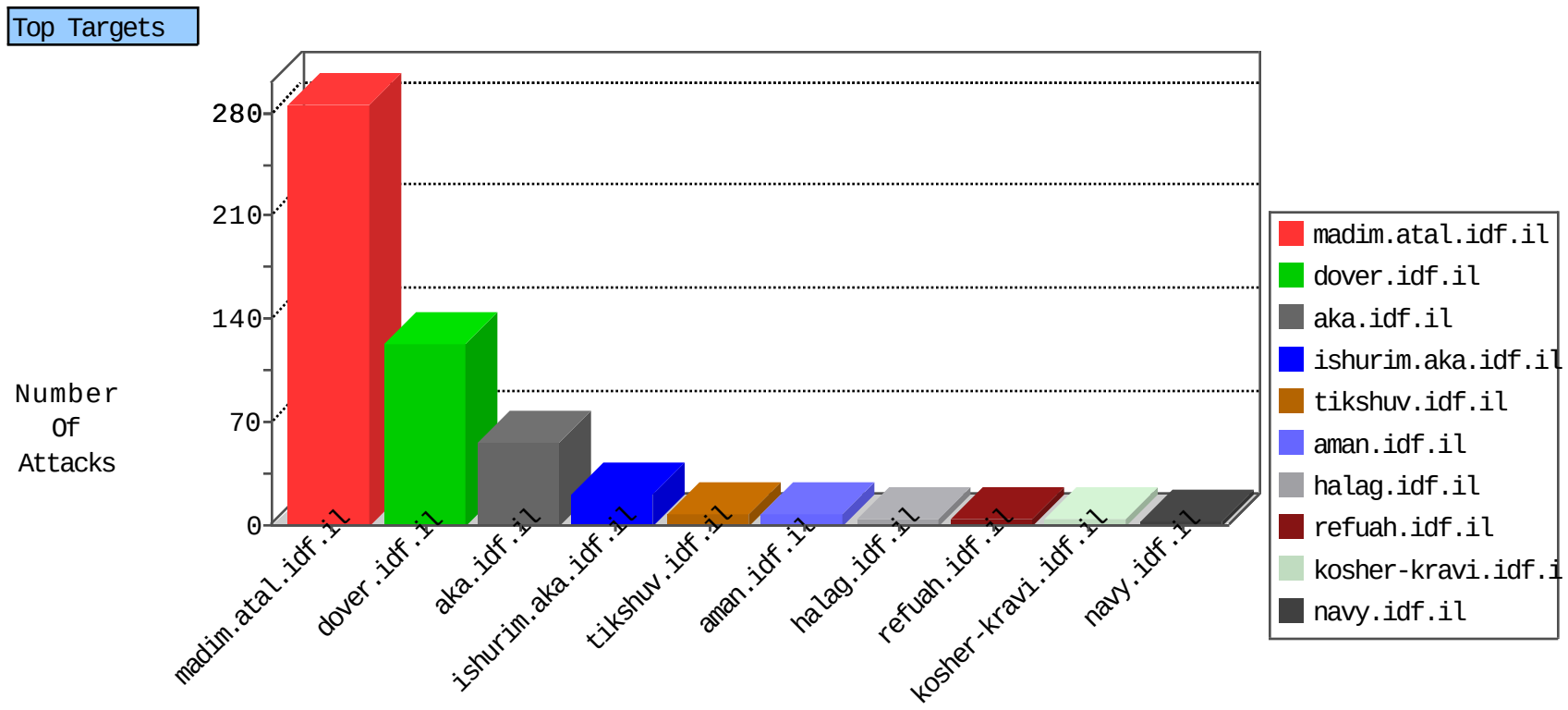
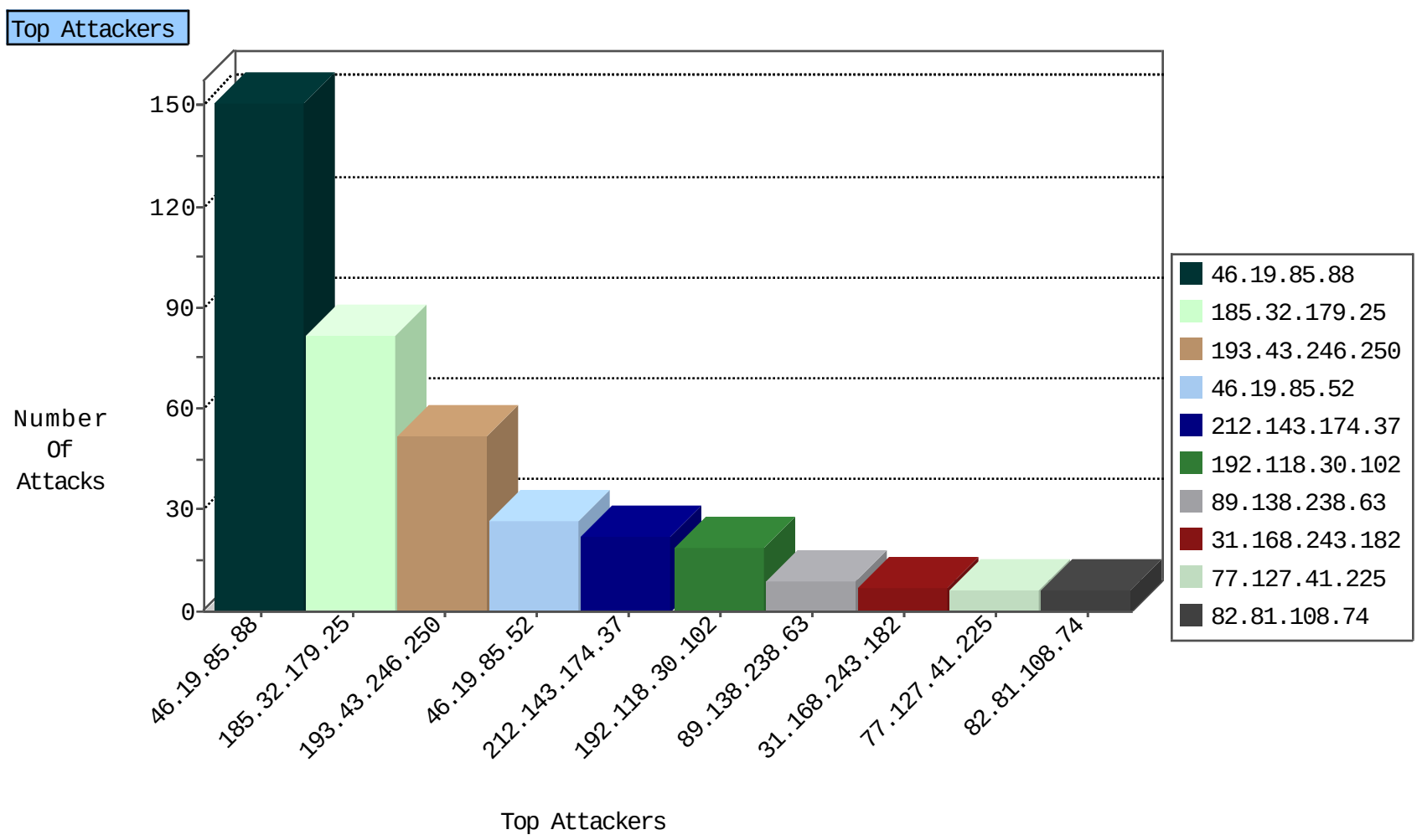
08-17-2016-12:04:01 to 08-17-2016-13:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-17-2016-12:04:01 to 08-17-2016-13:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.118.30.102	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
109.253.220.0	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
31.168.133.226	Israel	147.237.77.216	dover.idf.il	Black List	drop	2
93.158.200.131	Netherlands	147.237.76.34	yohalan.idf.il	Black List	drop	1
82.80.78.2	Israel	147.237.76.86	navy.idf.il	Black List	drop	1
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
89.248.171.2	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
201.166.236.206	Mexico	147.237.76.202	e.halag.idf.il	Black List	drop	1
58.218.204.245	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

08-17-2016-12:04:01 to 08-17-2016-13:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.149.126.98	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
174.34.135.242	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
123.126.68.127	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

08-17-2016-12:04:01 to 08-17-2016-13:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.125.184.101	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
80.246.137.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.81.215	147.237.77.216	Russian Federation	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.205.46	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.90.255.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.90.91	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.172.71.251	147.237.76.199	Ukraine	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
194.90.134.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
23.94.86.8	147.237.0.19	United States	madim.atal.idf.il	WEB-CGI redirect access	1
185.120.125.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.29.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
103.247.48.41	147.237.72.166	Sri Lanka	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN NMAP -f -sS	1
81.218.174.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.150.232	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.230.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.70.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.0.106.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.220.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.23	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.243.55.138	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.148.6	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.118.65.230	147.237.0.15	Russian Federation	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.50	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN NMAP -sS window 2048	1

08-17-2016-12:04:01 to 08-17-2016-13:04:01

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	52
212.143.174.37	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
77.127.41.225	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
82.81.108.74	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.168.243.182	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
212.143.174.37	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
80.179.192.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.203.236	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.200	m4u.idf.il	drop		drop	1
189.219.98.28	Mexico	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	1
109.253.144.159	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
169.229.3.91	United States	147.237.0.35	akaws.idf.il	drop		drop	1
216.243.31.2	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.145.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
187.160.83.159	Mexico	147.237.0.200	m4u.idf.il	drop		drop	1
109.253.146.247	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
212.143.174.37	Israel	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	1
187.185.131.211	Mexico	147.237.0.35	akaws.idf.il	drop		drop	1
109.190.4.90	France	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
201.172.68.143	Mexico	147.237.0.33	idf.il	drop		drop	1
109.253.158.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
31.168.243.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
212.185.61.13	Germany	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
189.215.92.143	Mexico	147.237.76.39	mobile.meitav.idf.il	drop	First packet isn't SYN	drop	1
109.253.128.116	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	151
185.32.179.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
46.19.85.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
89.138.238.63	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 89.138.238.63	Block	8
2.53.38.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
87.70.40.215	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	4
46.19.86.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.234.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.139.109.168	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunselectquestionnaire.aspx	Block	3
131.253.25.231	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
176.13.11.5	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	2
109.253.192.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.163	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/7/	Block	1
187.160.124.218	Mexico	147.237.77.176	matpash.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
169.229.3.91	United States	147.237.0.15	kosher-kravi.idf.il	NULL Character in Method	Block	1
201.172.155.121	Mexico	147.237.72.166	aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
187.160.183.109	Mexico	147.237.77.170	maarachot.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
77.125.15.252	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
62.219.242.101	Israel	147.237.77.234	halag.idf.il	Parameter Type Violation search in www.logistics.atal.idf.il/1213-he/halag.aspx	Block	1
40.77.167.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
207.46.13.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
109.66.133.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.243.55.134	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58339&docid=63703	Block	1
80.246.136.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19852-he/idfgdover.aspx	Block	1
187.160.182.80	Mexico	147.237.77.74	law.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method	Block	1
88.190.87.46	France	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 88.190.87.46 (Unsupported Cipher)	None	1
201.172.155.121	Mexico	147.237.72.167	ishurim.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
187.185.131.211	Mexico	147.237.0.34	tikshuv.idf.il	Redundant HTTP Headers Content-Type	Block	1
77.138.180.215	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/	Block	1
66.102.9.20	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.145	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.136	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/gallery	Block	1
84.94.210.34	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
187.160.183.109	Mexico	147.237.0.15	kosher-kravi.idf.il	Redundant HTTP Headers Content-Type	Block	1
176.13.9.248	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
2.53.36.170	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
201.175.104.139	Mexico	147.237.77.234	halag.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
189.218.109.163	Mexico	147.237.77.226	www.chamatz.aka.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
187.160.56.96	Mexico	147.237.77.233	atal.idf.il	Multiple Redundant HTTP Headers in header Content-Type	Block	1
66.102.9.31	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.85.52	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
212.143.174.37	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1